Woodland Primary School

E-safety Policy

Policy agreed by Governors: ……...18 June 2015

Lead Person ……..Jo Machon

Review Policy…… June 2016

1. Writing and reviewing the e-safety policy

Our e-safety policy has been written, following government and local authority guidance. It has been agreed by all staff and approved by governors.

- The E-Safety policy and its implementation will be reviewed annually.
- The E-Safety policy was written by: J Machon

Copies of the following documents should be read in support of this policy and can be found in the Administration Office or within staff shared documents on the main server:

- Health & Safety Policy
- Risk Assessments
- Recruitment & Selection of Staff / Volunteers
- Complaints & Disciplinary Policy
- Code of Conduct
- Diversity & Equality Policy
- Staff Induction / Development / Supervision Policy
- Confidentiality & Information Sharing
- Whistle Blowing policy
- Child Protection/Safeguarding Policy
- Behaviour policy
- PSHE policy
- ICT Acceptable Use policy

2. Teaching and learning

Why is Internet use important?

- The Internet is a part of everyday life for education, business and social interaction.
- Woodland Primary School have a duty to provide children and young people who show a responsible and sensible attitude towards it's use with Internet access.
- Children and young people use the Internet widely outside school and need to learn
- how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in Woodland Primary School is to raise educational standards, to promote pupil/children and young people's achievement, to support the professional work of staff and to enhance our management functions.

The benefits of internet use

- Access to experts in many fields for pupils and staff;
- Educational and cultural exchanges between pupils world-wide;
- Access to world-wide educational resources including museums and art galleries;
- 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;
- Access to learning wherever and whenever convenient.

Using the internet to enhance teaching and learning

- Children and young people will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Woodland Primary School will ensure that the copying and subsequent use of Internet derived materials by staff, children and young people complies with copyright law.
- Staff will guide children to on-line activities that will support the learning outcomes planned for their age and maturity.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating content

- Children and young people will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

3. Managing Internet Access

Information systems security

- The schools ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority and the school's IT support.
-

Managing filtering

- The school will work with LA and our internet service provider to ensure that systems to protect children are reviewed and improved.
- If adults or children discover unsuitable sites, the URL must be reported to the E–
- safety Co-ordinator: Miss H Kirk in Woodland
- Senior staff will ensure that regular checks are made to ensure that the filtering
- methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the organisation is allowed.

4. Privacy and Protection

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- **Any data containing 2 or more pieces of information about a child (first names, surname, date of birth, address etc. will be stored on the school system, on an encrypted memory stick/external hard drive, or transferred using It's Learning file share facility**.

Password security
Staff/volunteers will:

- Keep their password secure from others.
- Use a different password for accessing school systems to that used for personal purposes.
- Choose a password that is difficult to guess, or difficult for others to obtain by watching them login-adding numbers or special characters (*e.g.* !@£$%^) can help.

- Change passwords regularly.
- Will not write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- In addition, when leaving a computer for any length of time, all staff members/volunteers shall log off or lock the computer, using CTRL+ATL+DELETE or other system command.
- Always use their own personal logon, never using or sharing another persons logon details.

Pupils will:

- Foundation Stage and KS1 pupils will use a generic 'pupil' logon to all school
- equipment.
- At KS2 will have a unique, individually named user account and password for access to ICT equipment and information systems available within school.
- Be taught the importance of keeping their passwords secure, changing them regularly, or when they think someone else might know them and how to create a secure password (at least 8 characters, using numbers/letters/special characters)
- At KS2 always use their own personal logon to access computer systems.

Managing email

Approved protocol is:

initialsurname@schoolname.hull.sch.uk

- Children may only use approved email accounts.
- Children must immediately tell an adult if they receive offensive email.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Email sent to external organisations should be written carefully and, if it contains potentially contentious information, authorisation should be sought before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.

Managing published content

- The contact details on the website should be the school address, email and telephone number. Employee/volunteer or children's personal information must not be published.
- The appointed senior leaders will take overall editorial responsibility and ensure that content is accurate and appropriate.

Using images, video, sound and pupil's work

- Written permission from parents or carers will be obtained before photographs of children are published.
- Parents/carers can withdraw permission, in writing, at any time.
- Images that include children and young people will be selected carefully and will not enable individual pupils to be clearly identified.
- Children's full names will not be used anywhere on the website/Twitter, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of children are electronically published.
- Children's work can only be published with their permission or the permission of the parent/carer.
- Pupils and staff will only use school equipment to create images, sound and video.

- The school reserves the right to ask to see school equipment, including Ipads etc. at any time.
- Parents/carers may take photographs/videos of school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.

EYFS statutory framework

- Photographs/videos can only be taken with prior written permission.

Mobile phone use in school

- Mobile phones and personally-owned devices will not be used for personal use in any way during formal school times. They should be switched off or turned to silent.
- Mobile phones and personally-owned devices brought into school are the responsibility of the owner. The school accepts no responsibility.
- If mobile phones are used within lesson time as part of a curriculum based activity their use must be explicitly explained to the children.
- All mobile phones and personally-owned devices brought into school by the children must be handed in at reception.
- Staff will use a school phone where contact with pupils, parents or carers is required, unless the call needs to be made during an offsite activity.
- Staff should avoid using personal devices such as mobile phones and cameras to take photos or videos of children where possible. Where it is not possible to use a school device photos or video are taken the images must be downloaded and deleted as soon as possible.

EYFS statutory framework

- Mobile phones are not to be used in the rooms where children are cared for.

Social networking and personal publishing

- The Federation and our internet service provider will control access to social media and social networking sites.
- Staff and children will be encouraged to adopt safe and responsible behaviours in their personal use of social networking sites, blogs etc..
- Children will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messenger and email addresses, full names of friends/family, specific interests and clubs *etc*.
- Children will be advised on security and encouraged to set passwords, deny access
- to unknown individuals and instructed how to block unwanted communications.
- Children and young people should be encouraged to invite known friends only and deny accross to others by making profiles private.
- Children will be advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Children and parents will be advised that the use of social network sites is inappropriate for primary aged children.
- If pupils, parents or staff make inappropriate/offensive comments about the school, pupils, parents or staff then the school will seek advice on the best course of action to take and will then act on this advice.

5. Risks and Responses

Internet access

- The school will keep a current record of all staff/volunteers, children who are granted access to the Federation's electronic communications.
- All staff/volunteers must read and sign the Federation's policies regarding information security and the use of information technology before using the school's ICT resource.
- For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Children must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy.
- Parents/carers will be asked to sign and return a consent form for children's access.

Assessing risk

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit digital technology use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.

Handling complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

Managing Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in our policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by cyberbullying.
- All reported incidents of cyberbullying will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying:

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended for the user for a period of time.
- Parents/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

Children, staff and parents will be taught/made aware of the CEOP report button:

Child Exploitation and Online Protection (CEOP)
Children and young people need to know how to block someone online and report them if they feel uncomfortable. It is important to realise that there are people other than the staff in our school who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support. Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.

6. Communications plan

Introducing the policy to pupils

- KS2 pupils will be involved in creating and updating the E-Safety policy through discussions in class circles.
- E-safety rules and posters will be displayed in all networked rooms and discussed with children at the start of each year
- Children will be informed that network and internet use will be monitored.E-safety messages will be embedded across the curriculum whenever the internet or related technologies are used.
- E-safety is embedded within the ICT scheme of work
- Safer-Internet Day will be marked annually through assemblies and specifically planned lessons.

Introducing the policy to staff

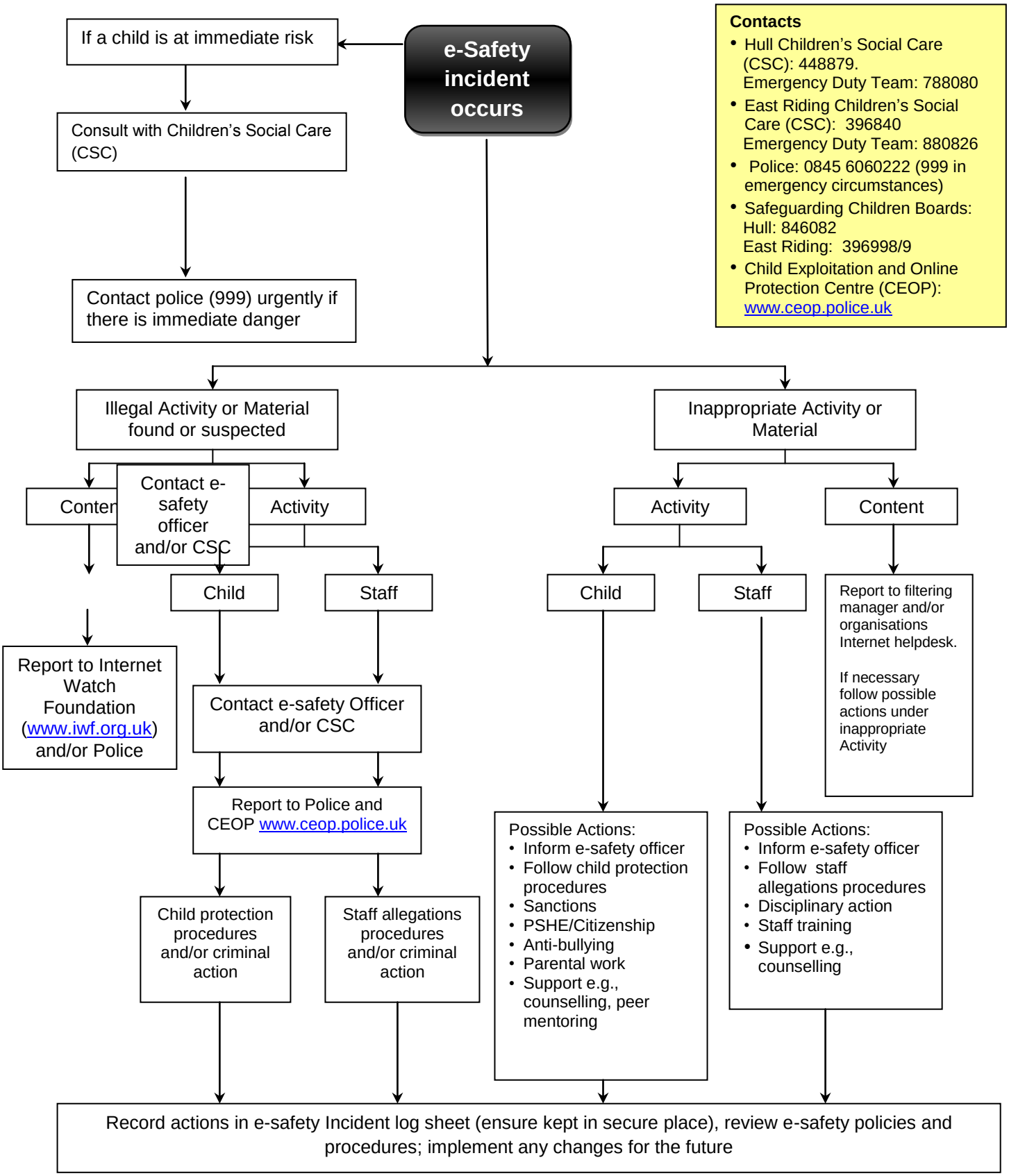
- The E–Safety policy will be formally provided to and it's importance explained to all members of staff.
- Staff will be required to sign an Acceptable Use Policy.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff may only use the internet for personal use outside of directed time (not within the hours of 8:45-12:00 and 1:00-3:15pm).
- Staff training needs will be audited annually and training provided to ensure up to date knowledge of e-safety and the safe and appropriate use of new technologies.
- Information regarding the safe use of new technologies will be shared with staff as appropriate e.g. Teacher tips for using Facebook

Enlisting parental support

- Parents'/carers' attention will be drawn to our E-Safety policy in newsletters, the school handbook and on each school's website.
- Parents will be involved in creating and updating the E-Safety policy through the use of questionnaires.
- Information regarding the safe use of new technologies will be shared with parents as appropriate e.g. Safer Facebook use

Response to Risk Flowchart

Response to and Reporting of an e-Safety Incident of Concern



Safety in a Digital World: Guide for Parents/Carers

You were taught road safety,

You were taught rail safety,

You were taught to play safely.

But now we are in the 21st Century and your children need to be taught e-safety

Children access the Internet on:

- **Computers**
- **Mobile phones**
- **Games consoles**
- **Music systems**
- **And they play games online with friends and *strangers***

They blog, chat, enter competitions, social network, email, watch TV online, download and upload information. They are creative at making music, making films and making web content.

Are you worried about their safety whilst accessing the internet?

This leaflet will provide you with some basic information to help you feel more confident in supporting your child to be e-safe.

The Benefits of Digital Technology

There are many benefits of having access to digital technologies. Here are some of them:

- Used effectively, these can improve children's achievement.
- Using them at home and at school develops skills for life.
- Children with supportive and involved parents and carers do better at school.
- Children enjoy using them.
- Using technologies provides access to a wider and more flexible range of learning materials.

Staying Safe

You can make a huge difference if you talk to your child about how they use digital technology, let them know you are there to guide them and pass on essential safety advice. Here are some do's and don'ts:

- Do keep your computer in a place where everyone can use it, go online with your child so you can see what they are doing on the internet.
- Do remind them that everyone they meet online is a stranger even though they might seem like a friend.
- Do encourage your child never to meet up with someone they make friends with online. But if they do then make sure they take along an adult you trust and to meet in a public place.
- Do explain that they shouldn't accept emails or open files from people they don't know. They may contain viruses, nasty messages or annoying links to things you don't want them to see.

- Do be aware that your child may as likely be a cyberbully as be a target of cyberbullying. Be alert to your child seeming upset after using the internet or their mobile phone.
- Do talk to your child so they know they can come to you if they run into any problems. Your continued involvement is the best way of keeping your child safe.
- Do make clear what content and behaviour is acceptable check that sites are age appropriate.
- Do give your child the knowledge and skills to build up resilience to the things they find online, help them to play and learn safely.
- Do consider using filtering software and agree ground rules about what services you are happy for your child to use.
- Do know how to complain.
- Don't allow them to give out personal information. That means full name, home or school address, telephone number or personal email or mobile number.
- Don't allow your child to access inappropriate sites.

If you want to find out more
A guide for parents about the potential dangers facing their children on the internet, plus advice on what parents can do to help counter these hazards:
www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety

Find the latest information on web sites, mobiles and new technology. Find out what's good, what's not and what you can do about it: www.thinkyouknow.co.uk

The UK Council for Child Internet Safety (**UKCCIS**) brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Safer Children in a Digital World consultation: www.dcsf.gov.uk/ukccis

Childnet International is a non-profit organisation working with others to help make the Internet a great and safe place for children: www.childnet-int.org

The Child Exploitation and Online Protection Centre (CEOP) works across the **UK** tackling child sex abuse and providing advice for parents, young people and children about internet safety: www.ceop.gov.uk

Or call 01482 616719 for further help and guidance.

Teach your child the internet safety code, Click Clever, Click Safe.

- **Zip It** – Keep your personal stuff private and think about what you say and do online.
- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments.
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.

Acceptable Use Agreement-Pupils

1. **I agree to keep my personal information safe**

2. **I agree not to access sites that are inappropriate for my age or download inappropriate content and I will tell adults about the sites that I am worried about.**

3. **I agree not to meet people without asking a parent/carer/adult.**

4. **I agree to report any worries I have to an adult and or use the CEOP report button.**

5. **I agree not to send rude or inappropriate messages, pictures or films.**

6. **I agree not to use digital technology to bully people or make threats.**

My child and I have read the acceptable use agreement for the safe use of ICT.

I understand that suitable guidance and supervision will be provided during times of internet access.

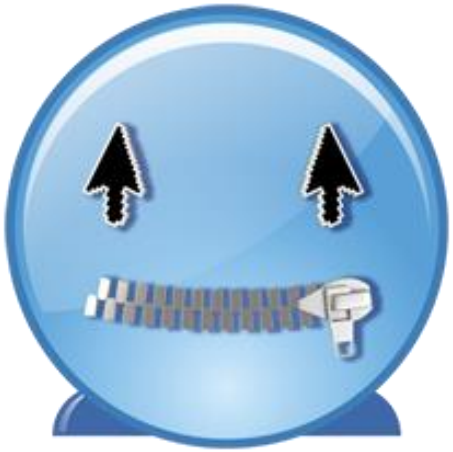
I give permission for my child to access the internet in order to enhance his/her curriculum.

Childs name: ……

Signed: ..... Date: .....

Remember the internet safety code. Click Clever, Click Safe

- **Zip It** – Keep your personal stuff private and think about what you say and do online .
- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments.
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.



ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.