Woodmancote School and Little Chestnuts
Online Safety Policy

Designated Member of Staff	S Perkins
Committee with responsibility	Safeguarding Committee
Date of Issue	March 2017
Frequency of Review	Yearly

Issue Number	Issue Date	Summary of Changes
1	March 2017	New Policy
2	May 2021	Updated roles and responsibilities

Introduction

The internet and other digital information technologies are powerful tools, which open up new creative ways for learning, communicating and working with others. As a school we believe that these new technologies have an extremely positive effect on the children that use them whilst in school and at home.

In order for every child to access these new technologies, there is a need for careful organisation on behalf of the school and a detailed policy which explains how they can be used appropriately and safely.

This policy seeks to explain clearly how this can be done and how school and home can promote online safety together.

Our aims:

- To help children to acknowledge the opportunities and the risks when working online.
- To develop a set of safe and responsible behaviours to support them whenever they are online.
- To help children understand what to do if they see something they don't like online.

Our duty:

- To teach children how to use new technologies safely.
- To ensure that this education should be appropriate to the children's age and level of skills and understanding.
- To instil within children a set of core principles to support them in their use of technology.
- To ensure that children become safe users of new technologies.
- To teach children how to stay safe both inside and outside of school.
- To teach children how to adapt to different technology uses as they grow older and technology (or exposure to technology) increases.
- To not detract from the fun and educational aspects of ICT.
- To ensure children are safe from terrorist and extremist material when accessing the internet.
- To give children advice and guidelines about what to do if they find something online that they are not sure about.

Online safety: Roles and Responsibilities

Governors

- Responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.
- Regular monitoring of online safety incident logs.
- Reporting to relevant Governors meetings.

Head Teacher

- Has a duty of care for ensuring the safety of members of the school community.
- Should be aware of the procedures to be followed in the event of a serious online safety allegation made against a member of staff.
- Responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues where relevant.
- Take a lead role in embedding safe internet practices into the culture of the school.
- Ensure that policies are current and adhered to.
- Implement an acceptable use policy to protect the interests of both pupils and staff.
- Draw links between this policy and other school policies, as appropriate, such as safeguarding and anti-bullying.
- Ensure that any breaches or abuse are monitored and reported.
- Ensure that all staff receive relevant information about emerging issues.

DSL

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying

Technical staff

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any LA online safety policies/guidelines.
- The filtering policy is applied and updated on a regular basis
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported for investigation.
- That monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Agreement (AUP).
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction.
- they ensure that all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites shecked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- To raise awareness of online safety issues among children including those of terrorist or extremist views.

Pupils (appropriate to age and level of skill and understanding)

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy, which parents / carers would sign on behalf of the pupils before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

- To play a crucial role in ensuring their child(ren) understand the need to use internet/mobile devices in an appropriate way.
- To endorse (by signature) the Pupil Acceptable Use Policy.

- Be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Understanding Risks

Alongside the positive educational benefits offered by digital technologies, there are some dangers, particularly for children. Whilst adult supervision of children's digital technologies use is preferable, it is not always realistic or practical, particularly outside school. We believe that it is necessary to alert children to the risks that they might encounter and help them to develop safe and responsible behaviours when using technologies, whether at school, at home or in any other setting. For children at Woodmancote School, certainly in the lower year groups, some of the risks might appear to be outside their level of ICT use. However, the children in our care engage with technology at an ever-younger age, and their knowledge and use of technological services, tools and devices can quickly outstrip that of their parents, carers and teachers.

In our school, although we are sensitive to the age and awareness of the children within our care: the core online safety message remains the same. The issues which we raise in school as part of this core message can be categorised into four areas: Content, Contact, Commerce and Culture.

Content

The Risks:

- When using the internet or other online service and technology, children may be exposed to inappropriate content.
- When accessing certain types of content, risks include viruses, adware and spyware.

Contact

The Risks:

- Fear of physical danger.
- Providing information whilst online that can be used to:
    - identify an individual or others
    - arrange to meet people that have been met online, thus posing a risk to an individual's safety or that of their family or friends.
- 'Cyber bullying' – an apparently anonymous method by which bullies can torment their victims. This may be in the form of email, chat or text messages.
- Extremist or radical views or opinions as in line with the prevent duty

Commerce

The Risks:

- When using new technologies, a child could do something that has financial or commercial consequences.

Culture

The solutions:

- Children need frequent education and guidance to embed and reinforce online safety messages so that they develop their own judgements of what is right and wrong and be better placed to remain safe wherever and whenever they use new technologies.
- Sharing information and details of good practice with parents. This will help to reinforce the work carried out in school and ensure that children receive consistent and comprehensive online safety advice.

Using the technologies safely

1. The internet

Background

- Enables users to obtain information and resources, to communicate with each other
- and to publish information
- Consists of a worldwide system of computer networks, in which users at any one computer can, if they have permission, access information made available on other computers.
- Vast amount of information available immediately.

Benefits

- Improved subject learning across a wide range of curriculum areas that promotes excellence, enjoyment and creativity, as well as independent learning through cross-curricular project work.
- Access to a wide range of cultural, scientific and intellectual material which might otherwise not be freely or readily available.
- Improved motivation and attitudes to learning.
- Development of problem-solving and research skills.
- Development of network literacy to access resources, create resources and communicate with others.
- Enhanced social development.

How will the Internet be used to enhance learning?

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be taught how to use the internet for research, including the skills of knowledge location and retrieval.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.
- Pupils will be taught how to recognise a reliable source and to think about what they reading on the internet in case they are reliable.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Curriculum Leader or Head Teacher.

The Risks

- Inappropriate content.
- Reliability, credibility and validity of information on some websites.

Strategies for safe use

Acceptable use policies (See Acceptable User Policy)

- Provides a framework for safe and responsible use of the internet.
- Provides guidance for pupils and parents using the internet at home.
- Outlines safe and responsible behaviours for pupils, procedures for reporting unsuitable material, and information on protecting the computer network.
- Covers a range of technology which might be used, both in and out of school, such as email, chat, instant messaging, camera phones, webcams, blogs and social networking sites.

Evaluating web materials

Pupils will be taught, at the right age, the value of critical evaluation as part if their core digital literacy skills development.

When evaluating materials, pupils should ask:

- Who has published the content?

- Where does the content come from?
- Does the content seem up to date?
- Is the content easy to read and understand?
- Does it present a one-sided point of view?
- Does the content provide everything I need?
- Are the links useful?

The Use of Filtering

It must be remembered that although filtering systems are effective tools, they are not 100% guaranteed. They must be supported by a safe and responsible approach to using the internet at all times.

- The school will work in partnership with parents, the Local Authority (LA), Department for Children Families and Schools (DCFS) and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing co-ordinator / Head Teacher.
- 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 must be referred to the Internet Watch Foundation.
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil.
- Children will be taught to use and respect the internet and other technologies at all times with clear sanctions being in place when either are misused.

How will the risks be assessed?

- 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 all reasonable precautions to ensure that users access only appropriate material. This includes using an Internet Service Provider which caters specifically for schools. 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 (though it is highly unlikely). Having taken reasonable measures, the school cannot accept liability for the material accessed, or any consequences of internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head Teacher will ensure that the Online safety Policy is implemented and monitored.

How will Internet access be authorised?

- The internet is seen as being an integral learning tool from the time that children start school. Younger pupils will be guided to using specific, age-appropriate websites. As the children progress throughout the school, they will be encouraged to use the internet independently but taught to discriminate their selection of relevant websites. Access to the internet will take place under adult supervision.

2. Using email

Background

- An effective way of sending messages over the internet.
- Attachments can include text, pictures, sound, animation or movies.

Benefits

- Develops communication skills and can transform the learning process.
- Encourages precision in spelling and choice of words.

Risks

- Open to abuse – Spam (unwanted email); 'Flaming' (angry or abusive emails); Bullying or harassment; 'Bombing' (a large email that is intended to crash a computer system); and Viruses.

Strategies for safe use

- As children progress throughout the school they will be taught about e-mail. Emails that are written should be written carefully and checked/authorised by the class teacher before sending.
- Children will be taught the importance of sending email to specific recipients and of the safe practices associated with email (no personal details).
- Children's use of email addresses to be limited to class or group with care being taken to ensure that individual pupils cannot be identified via their email address.
- Pupils must immediately tell a teacher if they receive unpleasant email.
- All mail that is sent to the school website will be checked before it is put on the school website.
- Children to be made aware of the characteristics of email bullying, the effects it can have on the recipient, and strategies for dealing with it. Sanctions will be put in place where it is clear that email is being misused, such as e-bullying.
- Email attachments will be treated with caution with a virus checker used on all outgoing and incoming mail, and always before opening and saving any attachment.

3. Using chat and instant messaging

Background

- A means of communicating with other people in real time over the internet in virtual meeting places called 'chat rooms'.
- Instant messaging – a form of online chat which is private between two people e.g Skype, Teams chat

Benefits

- Pupils are able to chat with their peers anywhere in the world
- Access to a wealth of information and experience

Risks

- Anonymity – one can never be sure who they are chatting to and the inherent risks attached to this.
- 'Cyber' bullying.

Strategies for safe use

- Pupils will not be allowed or be able to access chat-rooms or Newsgroups under any circumstances unless the service is provided through a suitable learning platform.
- Children made aware of the risks and ways of avoiding them.
- The implementation of an Acceptable User Policy.
- Keeping personal information private – name, age, location, extra curricular activities, names of friends (anything that could lead to an individual being identified or even contacted).
- If children are able to use chat-rooms away from school, they should only add people they know to their buddy list and should always use an instant messaging service which prevents others from adding their name to a buddy list without the owner's permission.

4. Using social software

Background

- The emergence of social media tools, or social software, which enhance or gain value from social interactions and behaviour. Examples of which include: 'Blogs' (weblogs) – the provision of an online diary or journal; 'moblogs' – blogs sent from a mobile phone; 'wikis' – modifiable collaborative web pages; 'podcasting' – subscription-based broadcasting over the web
- Social networking communities such as Facebook, Twitter, Instagram

Benefits

- New opportunities for personal expression.
- Delivering flexible and accessible online learning.

Risks

- Public spaces for both adults and children with published content which can be seen by a world wide audience.
- Publication of detailed personal information.
- Platforms for bullying, slander and humiliation of others.

Strategies for safe use

- Blocked school use of social networking sites
- Managed use of 'blogs' – teaching children effective communication skills against a backdrop of online safety.
- Teaching children how to be responsible publishers.
- Communication between home and school – Respecting age restrictions and the importance of keeping personal information private.

5. Using mobile phones and the mobile internet

Background

- Mobile phone use and ownership by young people is growing.
- SMS (Short messaging Service) – enables users to send and receive text messages,
- MMS (Multimedia Message Service – enables users to incorporate text, sound, images and video into their messages.
- 4G (fourth generation) with features such as digital cameras, mobile access to the internet and MP3 player.

Benefits

- Offer freedom, independence and a way to communicate to others.
- Safety – a young person can make contact and be contacted.

Risks

- Exposure to inappropriate materials.
- Physical danger – contact, content and crime.
- Cyber bullying.
- Legal, financial and commercial considerations.

Strategies for safe use

- Effective education about safe and appropriate behaviours.
- Keeping personal information private.
- The need to critically evaluate content.
- Blocking abusive messages.
- Immediately seeking help from a teacher, parent or carer if a child is bullied via mobile

phone.
- Seeking parental permission.

6. The School Website

Including images of pupils on the school website is a motivating experience for the pupils of the school and provide the school with an excellent opportunity to promote the varied and exciting work that is going on. It is crucial however that careful consideration is taken when deciding upon how images may be used.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press
    - Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
    - Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
    - Students/pupils must not take, use, share, publish or distribute images of others without their permission
    - Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
    - Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
    - Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

How will the policy be introduced to pupils?

- The development of a set of 'safe and discriminating behaviours' for pupils to adopt when using the internet and other technologies will be discussed with the children and reinforced. Instruction in responsible and safe use should precede internet access.
- Pupils will be informed that internet use will be monitored.
- Regular Online safety lessons in each year
- Regular Online safety assemblies using advice from Safer Internet Day and ThinkUKnow

Sanctions?

- Where misuse has occurred, judgement will be used by the class teacher, Computing Subject Leader, member of the Leadership Team or Head Teacher to ascertain whether the misuse was deliberate. Depending upon the seriousness of the offence, internal sanctions will be used. These may range from a first warning or to a temporary withdrawal of internet privileges. In extreme cases, parents or carers will be informed and access to digital technologies being withdrawn permanently.

How will staff be consulted?

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Online safety Policy, and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in the safe and responsible use of the internet will be delivered as part of the school programme for staff development.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Files held on the school's network will be regularly checked.
- The ICT Technician (Hardware) will ensure that the system has the capacity to take increased traffic caused by internet use. (currently using Focus Networks)

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to the Computing curriculum Leader and the Head Teacher.
- Any complaint about staff misuse must be referred to the Head Teacher or the Chair of Governors in more extreme circumstances.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions available include:
  - informing parents or carers;
  - interview with parent/teacher/Head Teacher;
  - removal of internet or computer access for a period of time.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Online safety Policy in newsletters, the

school prospectus and on the school website.

- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be developed and made available to parents.
- A stock of relevant leaflets from organisations such as British Educational Communications and Technology Agency (BECTA) and National Children's Hospital (NCH) Action for Children will be maintained.

Forging links between the Home and School

The school actively seeks to offer advice to parents related to the safe use of the internet at home. However, it is the individual responsibility of the parent or carers of the children to ensure that internet use is monitored closely. Parental attention will be drawn to such websites such as:

- Hector's World http://www.hectorsworld.com
- Kidsmart – http://www.kidsmart.org.uk/yp/under11

which are interactive websites which can be used to teach children to manage emails, respond to chat, evaluate websites and take part in an interactive quiz related to the safe use of the internet.

ThinkUKnow https://www.thinkuknow.co.uk/

Online safety resources (All available from a link on the school website)

CBBC – Own It	-	https://www.bbc.com/ownit/curations/staying-safe
Hector's World	-	http://www.hectorsworld.com,
Kidsmart	-	http://www.kidsmart.org.uk/yp/under11
Bullying Online	-	http://www.bullying.co.uk
Think U Know	-	http://thinkuknow.co.uk/
Common Sense	-	https://www.commonsensemedia.org/

Signed: …… Chair of Safeguarding Committee

Policies currently allocated to Safeguarding-December 2017
Acceptable Use
Anti-Bullying
Attendance
Behaviour
Children in Care
Code of Conduct
Complaints
Coronavirus
Online safety
Equality
Intimate Care
Medical Conditions
Positive Handling
Preventing Radicalisation
Recruitment and Selection
Safeguarding and Child Protection
SEN

Policies currently allocated to Premises-December 2017 which have a Safeguarding element
Accessibility Policy, Audit and Plan
Anaphylaxis Awareness and Monitoring
Disability Discrimination Policy and Plan
Business Continuity Plan
Emergency Asthma Inhaler Policy
Fire Risk Policy and Risk Assessments
Health and Safety Policy
Lone Working Policy
Lettings Policy
Off Sites Visits and Journeys
Security Policy
Records Management Policy