Online Safety & Anti-cyberbullying Policy

(In-line with ***Keeping Children Safe in Education 2020***)

Related Policies:

Behaviour Policy
Anti-bullying Policy
Safeguarding Policy
Equality Policy
Data Protection Policy

Policy Updated: September 2020
Future Review: September 2021

woodstock
CE PRIMARY SCHOOL

Nurture ~ Believe ~ Discover ~ Achieve

OUR CHRISTIAN VISION

Our vision for Woodstock CE Primary School reflects a passionate commitment to learning and recognition of the uniqueness of individual learners. Guided by our Christian values, it is driven by our desire to offer the best possible education for our pupils in partnership with parents, the Church and the local community.

Woodstock CE Primary School will be a centre for learning where adults and children:

- ✓ ***Nurture*** and prioritise wellbeing and development.
- ✓ ***Believe*** in themselves and in each other.
- ✓ ***Discover*** their own strengths and become successful lifelong learners.
- ✓ ***Achieve*** more than they ever thought possible.

OUR CHRISTIAN ETHOS

Recognising our historic foundation, we will preserve and develop our religious character in accordance with the principles of the Church of England and in partnership with the Churches at parish and diocesan level.

Woodstock CE Primary School strives to be an inclusive community where children grow, learn and achieve together. Within a nurturing, supportive and safe environment, mental health and wellbeing is at the heart of everything we do and recognised as the responsibility of all. Children's natural curiosity is fostered through a creative curriculum that excites and challenges, and enables them to be successful learners. Supported by a culture of equality and aspiration we aim to remove disadvantage so that every child can thrive.

We are committed to providing an education of the highest quality within the context of Christian belief and practice. We encourage an understanding of the meaning and significance of faith, and promote Christian values through the experience we offer to all our pupils.

"For I know the plans I have for you", **declares the Lord, "*plans to prosper you and not to harm you, plans to give you hope and a future.*"** Jeremiah 29, v11

woodstock
CE PRIMARY SCHOOL

Anti-cyberbullying Policy

CONTENTS

APPENDICES

1. Our Vision

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in E-safety can mean children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate pupils and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience.

'Our vision is to make the children at Woodstock School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'

Our policy and practice against this is clearly articulated in this E-Safety Policy.

2. What is E-safety?

E-safety is a school's ability to **protect and educate** a schools pupils and staff in their use of technology as well as having appropriate mechanisms in place to **respond** to, and support any incident where appropriate.

a. Protect

Protecting pupils means providing a safe learning environment by using appropriate monitoring and filtering to control what children can access while at school. But, this only protects them while they are on school premises. Education around e-safety is the only way to ensure that, wherever they are, they know how to stay safe online.

b. Educate

Learning about e-safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, or mitigate the possibility of risk.

The School's E-safety curriculum is progressive and covers a wide range of aspects, including:

- Online behaviour – understanding what constitutes cyber-bullying, inappropriate content and sexting, how to behave safely and with respect for others.
- Protecting your online reputation – understanding both the risks and rewards of sharing personal information online (your digital footprint).
- Learning to evaluate internet content – understanding how to research, evaluate and use published material

c. Respond

Responding to issues is both about ensuring pupils know what to do if anything happens to put their online safety at risk, and taking direct and immediate action as a school where incidents occur.

Woodstock CE Primary School has clear and robust policies and procedures to identify and immediately respond to e-safety risks or incidents, efficiently and consistently. It is important to note that the school's remit to act goes beyond the classroom, to regulate pupils' conduct and safeguard them when they are not on school premises or under the lawful charge of school staff.

3. Why use the internet for Teaching and Learning?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

The rapid developments in electronic communications are having many effects on society. Only ten years ago we were asking whether the Internet should be used in all schools. Now, it is an essential aspect of learning across all walks of life. In school, access to the internet is essential to:

- Raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.
- Prepare children and young people for life in 21st century in terms for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Teach pupils how to evaluate Internet information and to take care of their own safety and security rather than be sheltered from potential risks.

There are many benefits of the Internet to learning:

- Access to world-wide educational resources
- Collaboration and communication between pupils
- Access to anytime, anywhere learning
- Educational and cultural exchanges between pupils world-wide to develop global understanding
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and example of effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of information

With increased use of the Internet, protecting and educating pupils to manage the risk becomes our primary concern. As a school we commit to provide parents with support and information in keeping children safe online.

4. Who does this policy cover?

There are multiple groups that are impacted by this Policy. They are:

- Pupils
- Staff
- Parents
- School Governing Body

a. Pupils

A pupil's perceptions of risks will vary; the school has a clear Code of Conduct for Responsible Use of Technology which is developed and agreed by staff and pupils together. To support appropriate access to the Internet and use of electronic communications, we ensure that:

- The E-safety Policy is summarised to, and discussed with our Children's Council and their comments invited.
- The E-safety Responsible Use Policy is shared with pupils, and parents are encouraged to discuss and emphasise the Policy for home use.
- The E-safety Code of Conduct is clearly posted in all networked rooms.

- Pupils are frequently informed that Internet use is monitored.
- A professionally led E-safety training programme is delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools. This programme is delivered in the classroom through Computing skills lessons and PSHE sessions, and beyond the classroom through structured annual training and specially focussed assemblies. E-safety messages are re-enforced each time Internet access or ICT usage is given.

b. Staff and Volunteers

Woodstock CE Primary School E-safety Policy will only be effective if all staff, and support volunteers subscribe to its values and methods. As standard practice we ensure that:

- All staff are given the School E-safety Policy and its application and importance explained.
- Staff & volunteers are asked to read and sign in agreement to the 'Staff Acceptable Use Policy'
- Staff are fully aware that Internet traffic can and will be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The E-safety & Acceptable Use Policies are a core part of the induction programme for any new staff and volunteers.
- Training for teaching and non-teaching staff in safe and responsible Internet use and on the school E-safety Policy is provided regularly. Classroom practice is monitored periodically to ensure effective compliance.

c. Parents

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unintended unrestricted access to the Internet. As a school, we recognise the importance of striking a careful balance between informing and alarming parents. Our policy is to:

- Draw parents' attention to E-safety resources in particular the school's E-safety Policy, relevant articles and resources from trusted sources, and online reporting procedures in newsletters and on the school website.
- Handle internet issues sensitively, to inform parents without alarm.
- Encourage a partnership approach with parents where careful and informed practise can be supported in and out of school. This includes professionally delivered parent E-safety information evenings that build awareness of benefits and risks, and offer independent advice and best practice suggestions for safe home Internet and e-communications use.

d. School Governing Body

All Governors of the school are expected to understand, uphold and ensure e-safety best practice for staff and pupils. As Internet and communications access broadens, so governors must ensure that the school keeps pace in its policies and procedures and can effectively protect, educate and respond. To support this, we ensure:

- ICT and E-safety are a core part of our School Raising Achievement Plan. A nominated E-safety governor is responsible for ensuring effective practice and partnering progress towards agreed commitments and targets. Commitments and process are reviewed by the full Governing Body every term.
- All Governors receive professionally delivered E-safety training alongside staff and are clear as to their role in due diligence.
- All Governors receive an E-safety Report outlining implemented practices and reported incidents each term.
- Governors are able to play a role in extending our E-safety reach into the wider school community.

As a School we have formed an E-safety Committee which consists of members from all of these stakeholder groups as well as representation from external E-safety and ICT experts.

5. Policy

a. Cyber Bullying

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and un-intended involvement an increased risk. Woodstock CE Primary School has a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) is given as part of an annual Anti-bullying Week and E-safety Day.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff, who have a range of materials available to support pupils and their families.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our Anti-bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

b. Grooming

Grooming is a word used to describe how people who want to co-opt or potentially harm children and young people get close to them, and often their families, and gain their trust. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect pupils against this risk. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards. No mobile phones.
- All online access and pupil generated content in school is monitored and password protected.
- Pupils are taught how to behave responsibly on line and the 'golden rules' in protecting personal information. More information is outlined in Section 7 of this Policy: Behaviours.
- Pupils, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe on line.

c. School Managed Content and Authorised Access

Woodstock CE Primary School has very clear measures and controls in place to enable responsible Internet access and usage. These are outlined as a key part of this E-safety Policy, as below:

Authorising Internet Use:

At Woodstock Primary School pupil usage is supervised, with access to specific approved online materials. Pupils are authorised to access the internet as a group or independently, depending on the activity. All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource and parents are equally requested to share the Acceptable Use Policy with their children.

In order to be granted Internet access, pupils must complete the E-safety Code of Conduct for Responsible Use of Technology form. A list of children without permission to use the Internet is kept in the school office and is known to teaching staff.

Managing Filtering:

Whilst levels of Internet access and supervision will vary according to the pupils' age and experience, our policy is that Internet access must be appropriate for all members of the school community. Our Internet connection was arranged by IT support company 123 ICT following advice from Oxfordshire County Council and provision is through Schools Broadband, a specialist division of Talk Straight Ltd, a leading telecommunications provider in the UK. Our Broadband

is received by a dedicated Internet connection and is tailored with filters to our specific needs. The procedures for ongoing management and review are:

- The school will work with Schools Broadband and 123 ICT to ensure that systems are reviewed and any improvements are implemented.
- If staff or pupils discover unsuitable sites, the URL must be reported to a member of the 123ICT team who will then ensure that the URL is blocked.
- Any material that the school believes to be illegal must be reported to appropriate agencies (IWF or CEOP)

Managing E-mail and Communications:

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits.

Staff: All staff are given a secure school e-mail address upon joining the school. The creation of these accounts is the responsibility of the school's Business Manager. Should any staff need to contact parents directly then they should use their school e-mail, or if relevant, the school mobile, otherwise all communications should be passed on by the school office. All personal contact details for staff members will remain private.

Pupils: In certain circumstances pupils may be given access to an approved Office 365 email account. This is likely to be in the context of a class email address rather than an individual email account.

In order to enable responsible and safe e-mail use, the following measures are in place:

- Pupils may only use approved Office 365 e-mail accounts.
- Pupils only have access to internal e-mail to teachers and fellow pupils.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Use of words included in the filtering/checking 'banned' list will be detected and logged.
- Pupils are taught how to use e-mail during Computing skills lessons from Year 1 upwards and educated in the risks and how best to manage them.
- Access in school to external personal e-mail accounts may be blocked by the School's Broadband filtering systems.
- The school reserves the right to monitor user's e-mail accounts provided by the school.
- Outside school pupils are advised not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Password Protection:

Upon joining the school, the system administrator creates a unique username and generic password for each child that they can use to log into the school's network. The children's passwords can be reset and changed by the system administrator using a networked device.

In Key Stage 1, the children do not change their default password and the class teacher keeps a record of their log-in details. In Key Stage 2, the children are asked to change their passwords, choosing one that they will be able to remember. Their class teacher will also keep a record of their changed log-in details. As part of computing lessons and E-safety teaching, children are taught about the importance of keeping their personal details, including passwords, private.

Managing Published Content and Images:

Our school website celebrates pupils' work, promotes the school, publishes resources and acts as a communication tool. Publication of information on the Woodstock CE Primary School website is carefully considered from a personal and school security viewpoint.

Contact details available on the website are school address, e-mail and telephone number. Staff or pupils' personal information must not be published and all images used will comply with the conditions below:

- Children's names are published as their first name only e.g. Trevor, or if required, first name and last name initial e.g. Graeme B.
- Adults may be referred to by their full name, but only with their agreement.
- Any images of children must **not** be labelled with their names.
- Children will only be shown in photos where they are suitably dressed.
- Completed consent forms from parents or carers must be obtained before images of pupils are electronically published. A master list is available and updated by the school office staff.
- While images may be taken by parents, it is requested that they are not shared in the public domain.
- All digital images are securely stored and disposed of in accordance with the Data Protection Act.

Managing Information Services:

Woodstock CE Primary School commit to take due care in regard to managing the provision of Information Services to support secure and appropriate access. The measures outlined in this Policy include:

- Network servers are kept securely in a locked room.
- The security of the school information system is reviewed regularly 123 ICT and Talk Straight Ltd.
- The school keeps the network secure with a number of group policy settings and permissions which only allow certain users to use portable storage devices and to access and open certain drives and files.
- The school reserves the right to monitor user areas and equipment provided by the school.
- Sophos anti-virus software updates automatically every hour. Staff are also encouraged to install Sophos at home to increase security.
- The school uses Internet firewall and filters provided by Talk Straight Ltd.
- For fire safety network server backups of user data are taken daily and stored remotely using online servers.

d. Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. There is increasing educational potential of such tools, for example in the use of blogs and wikis to improve writing.

However, whilst direct access to social networking sites in school is limited and regulated, a significant number of pupils in upper KS2 now use social networking out of school hours on a regular basis. As a school, we recognise that they may need guidance and support in knowing how to stay safe in such sites, and parents may not know what advice to give them. Pupils need to be encouraged to consider the implications of uploading personal information and the relative ease of adding the information and the practical impossibility of removing it.

Pupils need to be taught the reasons for caution in publishing personal information and photographs on the Internet and in particular on social networking sites. Our E-safety Policy aims to provide guidance and council on keeping safe within social networking and personal publishing. Specific council is:

- Within school hours, the school blocks access to social networking sites unless a specific use is approved.
- Pupils are 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,
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff must ensure their profiles on social networking sites are private and not to add past or present pupils as friends.
- Staff should not give out their personal email address to parents. All communications must go through the school office.

- Staff and pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others. They are advised not to publish specific and detailed private thoughts.

We very much acknowledge that we cannot act in isolation and parent's co-operation in supporting these steps is greatly appreciated.

e. E-Safety Complaints

For safe practice to be a reality, pupils, teachers and parents must know how to submit a complaint. The Complaints Policy is available on the school website and in paper form from the school office. If parents, pupils or members of the public have concerns they should:

1. Discuss their concerns with the member of staff most directly involved and, if not satisfied;
2. Discuss their concerns with a senior member of staff and, if not satisfied;
3. Discuss their concerns with the Headteacher. If the Headteacher considers she can do no more to resolve the complaint it will be stated explicitly that the complainant can write to the Chair of Governors if not satisfied.

Complainants are encouraged to state what actions they feel might resolve the problem at any stage.

Prompt action will be taken if a complaint is made. A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's Disciplinary Policy.

Formal complaints of Internet misuse will be dealt with by a member of the Leadership Team. 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.

Only where all these avenues have been tried and found unsatisfactory should the complainant take a complaint to the Chair of Governors or Clerk to the Governing Body.

f. Risk Assessments

In-line with commitments made within this Policy, 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 appear on a school computer. All Internet access at Woodstock CE Primary School is filtered through the LA filtering system. Whilst very robust in their practises around Internet use, neither the school, 123 ICT nor Schools Broadband can accept liability for the material accessed, or any consequences resulting from Internet use.

In order to ensure that risk is minimised, the following actions are taken:

- Methods to identify, assess and minimise risks are reviewed regularly.
- Staff, parents, governors and advisers work to establish agreement that every reasonable measure is being taken.
- Pupils are taught to consider the risks of using the Internet and how best to manage them.
- The Headteacher will ensure that the E-safety Policy is implemented and compliance with the Policy monitored.

6. Guidelines by Technology

The Policy is applied across a range of technologies that continue to expand and evolve. In addition to computers and tablet devises commonly used to access the Internet or enable communications, this Policy outlines clear guidelines as they apply to other known and used technologies. Specifically:

a. Video Conferencing

Video conferencing, including Skype and FaceTime, enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education. The practices below aim to ensure that we apply our e-safety commitments to video conferencing.

Equipment:

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP video conferencing must use the educational broadband network to ensure quality of service and security rather than the Internet.
- Video conferencing contact information will not be put on the school website
- The equipment must be secure and locked away when not in use.

Users:

- Video conferencing will be supervised by an appropriate adult at all times.
- Pupils must ask permission from the teacher before making or answering a videoconference call.

Content:

- When a lesson is to be recorded, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of video conference must be clear to all parties at the start of the conference.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, checks will be made to ensure that they are delivering material that is appropriate for the audience.

b. Internet enabled mobile phones and handheld devices

Increasingly, a greater number of young people have access to new and sophisticated Internet-enabled devices such as SMART mobile phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Our policy is that pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

However, in acknowledgement of the growing use, pupils will be taught about the benefits and risks, the legal and moral implications of posting photos and personal information from mobile phones to public websites, and how the data protection and privacy laws apply.

c. Online Gaming

Online gaming can be a helpful and engaging way of developing learning through play with a range of educational content presented through games to support literacy, maths, problem solving, strategy or coding. Controlled use may be supported within the classroom but always through screened individual log-in programs or via teacher lead activity where fit for use and appropriate access settings have been pre-assessed.

However, we also recognise from our recent Internet Survey that gaming plays a key part in recreational play in the home setting or when with friends. We have therefore outlined some best practice guidance from Microsoft which will help to support and keep children safe when gaming online.

Making safe choices:

All games all have age guidance ratings so that content can be assessed as appropriate. Check the ratings of the games your children want to play. In the UK most games for consoles or online have a PEGI rating which can be found on pack or searched for via the PEGI website. You can use these ratings as you discuss the most appropriate games with your child. In line with our safeguarding policy we would look to protect children from content that is violent or inappropriate by advising strongly that children are not permitted access to games with a PEGI rating greater than 7.

Beyond the content rating, selecting games that are well-known or those from reputable sites will reduce the risk of downloading viruses or sharing data in an unprotected way. You can also review the game's terms of play to find out how the game service monitors players and responds to abuse and read the site's privacy policy to learn how it will use and protect children's information.

Being aware of the risks:

Games that have no on-line connection, no entry of personal data or passwords and that are user only controlled do not pose a potential e-safety risk, however, to add an extra dimension to a game there is increasingly a multiplayer element, where players often communicate via integrated chat or verbally with microphone or a headset.
Many games – from simple chess to first-person adventure games, where thousands of players participate at the same time – include these features. The presence of such a large online community of anonymous strangers and the unfiltered, unmoderated discussions, can pose a variety of potential risks such as:

- Inadvertently giving away personal information, including password, email or home address or age.
- Inappropriate contact or behaviour from other gamers
- Buying or selling virtual, in-game property – for example high-level characters – where there is real money involved.
- Disposing of game consoles, PCs and mobile devices without deleting your personal information and account details.
- Playing games for many hours at a time with the danger of becoming addicted.

Recommended solutions:

Gaming can be an enriching learning experience with some simple steps to keep safe:

- Play online games only when you have effective and updated antivirus software and firewall running.
- Play only with authorised versions of games which you have purchased from the correct sources and for which you have a license. Verify the authenticity and security of downloaded files and new software by buying from reputable sources.
- Choose a user name and password with your child that does not reveal personal information. Similarly, if the game includes the ability to create a personal profile, or where contact can be made by other players make sure that no personal information is given away.
- Read the manufacturer or hosting company's terms and conditions to make sure there will not be any immediate or future hidden charges.
- When disposing of your gaming device either by selling, scrapping, giving away or donating, ensure all of your personal information and your account details have been deleted.
- Set guidelines and ground rules for your children when playing online. This could include time limitations, parent entered passwords or game play only in communal areas

d. Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology, and effective practice in classroom should be developed. The contents of this Policy are regularly reviewed and updated in light of the on-going changes to modern technologies.

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

7. Behaviours & Sanctions

A critical part of our E-safety Policy which applies across all technologies are the behaviours we seek to embed and the sanctions pupils or staff may face if their actions put their or others E-safety at risk.

Behaviours

Personal Information is Personal

Pupils learn to never give out personal details such as name, address, date of birth, school
User names and passwords should not contain personal information

Treat others online as you do in the real world

Pupils learn that online bullying and harassment are potential problems that can have a serious effect on children. They are aware that causing upset or harm online will follow the same sanctions as outlined in our

Strangers Online are still strangers

Pupils learn to recognise that friends are people we know and see regularly as part of our everyday lives. Online "friends" are strangers and invitations to meet them in the real world should be reported.

Evaluate what you see and do

Pupils learn to evaluate everything they read, and to refine their own publishing and communications with others via the Internet. They are supported in learning to evaluate internet content as outlined in the section

What to do if something isn't right

Pupils learn that if they know or feel something isn't right that they should speak to, or contact an adult immediately.

Sanctions:

The school would take immediate action if pupils or staff were to put themselves or others at risk. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

Pupils: Sanctions within the school Behaviour Policy will apply:

- Interview/counselling by a member of the Leadership Team
- Informing, and if appropriate, meeting with parents or carers
- Removal of Internet or computer access for a period.

Staff: As a school we have formally adopted Oxfordshire County Council's Discipline Procedures for all Employees in Schools. It is essential for staff to use the Internet, including social media in a responsible and professional manner both in school and out of school, in order to ensure the privacy and safety of all employees, pupils, parents and members of the wider school community.

Effective support, supervision and counselling of staff by a member of the Leadership Team should reduce the need to use the disciplinary procedure. Incidents relating to irresponsible Internet use will be brought to the employee's attention as soon as possible in an effort to resolve the situation informally, however if appropriate more formal procedures will be set in motion in-line with OCC guidance.
Any incidents will be reflected on by the E-safety Committee and retraining organised if appropriate.

8. Learning to Evaluate Internet Content

Developing best practice Internet use is imperative. Parents and teachers can help pupils learn how to distil the meaning from the mass of information provided on the Internet.

Often the quantity of information is overwhelming and staff guide pupils to appropriate websites, or teach search skills. Information received via the Internet, e-mail, or text message requires good information handling skills. Our approach is to offer younger pupils a few good sites as this is often more effective than an Internet search. Respect for copyright and intellectual property rights, and the correct use of published material are taught.

Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet. Specifically:

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity.
- ICT skills lessons are used to educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. This is reinforced by teachers when using the internet within their classroom.
- The school ensures that copying and subsequent use of the Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

9. Protecting Personal Data (GDPR)

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

Please refer to our school GDPR Policy and Guidance documents which can be accessed via our school website for further information on this.

Introduction

The school recognises that technology plays an important and positive role in everyone's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

Aims

The aims of this policy are to ensure that:

- We safeguard the pupils in the real and virtual world
- Pupils, staff and parents are educated to understand what cyberbullying is and what its consequences can be
- Knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community
- We have effective measures to deal effectively with cases of cyberbullying
- We monitor the effectiveness of prevention measures

What is Cyberbullying?

Cyberbullying: A Definition

Bill Belsey, the creator of the web site: http://www.cyberbullying.org/ defines this unpleasant and particularly intrusive phenomenon in the following terms:

> ***"Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others."***

Cyberbullying can involve Social Networking Sites, emails, mobile technologies used for messaging and as cameras. In addition:

- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying
- It can also go further in that it can invade home/personal space and can involve a greater number of people
- It can take place across age groups and school staff and other adults can be targeted
- It can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'cyberstalking'; vilification/defamation; exclusion or peer rejection;
- Impersonation; unauthorised publication of private information or images ('happy-slapping'); and manipulation
- It can be an illegal act

Preventing Cyberbullying

Understanding and Discussion

- Staff receive training in identifying cyberbullying and understanding their responsibilities in developing e-safety. In this training all staff will be helped to keep up to date with the technologies that children are using.
- The delivery of PSHE and general ICT lessons are an important part of preventative strategy and will discuss keeping personal information safe and appropriate use of the internet.
- It is desirable that the pupils will be involved in a response to cyberbullying. They will have a voice through the School Council.
- Pupils will be educated about cyberbullying through a variety of means: assemblies, conferences, Anti-bullying Week, projects and our annual Safer Internet Day.

- Pupils will sign a Safe and Acceptable Use Policy before they are allowed to use school computer equipment and the internet in school and parents will be encouraged to discuss its contents with their children.
- Parents will be provided with information and advice on e-safety and cyberbullying via literature, talks, etc.

Policies and Procedures

- Ensure regular review and update of existing policies to include cyberbullying where appropriate, through our E-Safety Committee
- We will keep good records of all cyberbullying incidents. All staff are responsible for reporting all incidents to the Headteacher or E-Safety Lead.
- The Business Manager keeps all AUP records
- Publicise rules and sanctions effectively
- The school (with the support of our 123ICT Technician) ensures the effective use of filtering, firewall, anti-spyware software, anti-virus software and secure connections to safeguard the pupils. Though electronic controls alone can never be 100% effective, and pupils should adhere to the AUP guidelines

Promoting the Positive Use of Technology

Woodstock Primary School will;

- Make positive use of technology across the curriculum
- Use training opportunities to help staff develop their practice creatively and support pupils in safe and responsible use
- Ensure all staff and children understand the importance of password security and the need to log out of accounts

Making Reporting Easier

- Pupils may speak with any staff member when they are concerned about a bullying issue
- Ensure staff can recognise non-verbal signs and indications of cyberbullying with regular safeguarding training.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement
- Publicise to all members of the school community the ways in which cyberbullying can be reported
- Provide information for all pupils including reassurances about 'whistleblowing' and the appropriate way of informing appropriate staff or parents about incidents they have witnessed
- Provide information on external reporting routes e.g. mobile phone company, internet service provider, Childline, CEOP or the NSA

Evaluating the Effectiveness of Prevention Measures

- Identify areas for improvement and incorporate pupil ideas derived from School Council meetings.
- It is desirable to conduct an annual evaluation including a review of recorded cyberbullying incidents.

Responding to Cyber bullying

Most cases of cyberbullying will be dealt with through the school's existing Anti-bullying Policy and this must remain the framework within incidents of bullying are investigated. However, some features of cyberbullying differ from other forms of bullying and may prompt a particular response.

The key differences are:

- Impact: the scale and scope of cyberbullying can be greater than other forms of bullying
- Targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets
- Location: the 24/7 and anywhere nature of cyberbullying
- Anonymity: the person being bullied will not always know who is bullying them
- Intent: some pupils may not be aware that what they are doing is bullying
- Evidence: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence
- It is possible that a member of staff may be a victim and these responses apply to them too

Support for the Person Being Bullied

- Offer emotional support; reassure them that they have done the right thing in telling someone
- Advise the person not to retaliate or reply. Instead, keep the evidence and take it to their parent or a member of staff (in the case of staff they should take it to the Headteacher or E-Safety Lead)
- Advise the person to consider what information they have in the public domain
- Unless the victim sees it as a punishment, they may be advised to change e.g. mobile phone number
- If hurtful or embarrassing content is being distributed, try to get it removed from the web. If the person who posted it is known, ensure they understand why it is wrong and ask them to remove it. Alternatively, contact the host provider and make a report to get the content taken down
- In some cases, the person being bullied may be able to block the person bullying from their sites and services

Investigation

- The safeguarding of the child is paramount and staff will investigate in accordance with the Woodstock CE Primary School's Safeguarding and Child Protection Policy (this can be found on our school website)
- Members of staff should contact the Headteacher/E-Safety lead in all cases
- All cases (including Child Protection issues) will be referred to and logged by Headteacher
- Interviews will be held in accordance with the Woodstock CE Primary School Anti-bullying Policy
- Staff and pupils should be advised to preserve evidence and a record of abuse; save phone messages, record or save-and-print instant messenger conversations, print or produce a screenshot of social network pages, print, save and forward to staff whole email messages
- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact the Headteacher (DSL), who may involve appropriate external agencies, the local police in cases of actual/suspected illegal content, or CEOP http://ceop.police.uk
- Identify the bully
- Any allegations against staff should be handled as other allegations following guidance in 'Keeping Children Safe in Education'
- Confiscate device(s) if appropriate

Working with the Bully and Applying Sanctions

Sanctions will be applied by the Headteacher as appropriate.

The aim of the sanctions will be:

- To help the person harmed to feel safe again and be assured that the bullying will stop
- To hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour
- To demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly
- Sanctions for any breaches of AUPs or internet/mobile phone agreements will be applied
- In applying sanctions, consideration must be given to type and impact of bullying and the possibility that it was unintentional or was in retaliation
- The outcome must include helping the bully to recognise the consequence of their actions and providing support to enable the attitude and behaviour of the bully to change
- A key part of the sanction may well involve ensuring that the pupil deletes files

Legal Duties and Powers

- The school has a duty to protect all its members and provide a safe, healthy environment
- School staff may request a pupil to reveal a message or other phone content and may confiscate a phone
- If they consider that a mobile phone may contain evidence of bullying or a crime or the potential of a crime they may investigate the specific contents relating to that act;
- Some cyberbullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997.

For further references please refer to the Woodstock CE Primary School Anti-bullying Policy and the Safeguarding and Child Protection Policy (both can be accessed via the Policies page of the school website).

General Advice on Protecting Yourself Online and Dealing with Cyberbullying

To avoid the risk of being exposed to illegal content and protecting yourself online, we recommend the following precautions:

- Do not share your personal information! This includes pictures of you or your family and friends, email addresses, mobile numbers and online IDs.
- Do not arrange to meet strangers! You may have been communicating with people you think you know online, but do you really know who they are?
- Do not open email or links on social networking pages from people you do not know or when you do not recognise the email address
- Similarly, do not open attachments or pictures you receive from unknown people or email addresses
- Ensure you have an effective filter on your PC to stop unwanted content.
- If you are regularly using search engines (such as Google, Bing or Yahoo), you can set each search engine site to a strict level of filtering. This limits what a search will bring up when entering keywords. Check your options with your preferred search engine site. Once you have chosen a search filtering level, check these settings regularly to ensure they have not been amended or switched off.
- Viewing illegal images online can carry a penalty of up to 10 years in prison in the UK.
- Curiosity is normal on the internet but being exposed to unwanted and potentially illegal images is not acceptable.
- Child Abuse images reflect just that; abuse of children and as such, should always be reported.
- Did you know that the age of criminal responsibility starts at age 10 in England and Wales!

General advice on how to deal with Cyberbullying

Due to the anonymous nature of digital communication, anyone with a mobile phone or internet connection can be the target of cyberbullying. Our schools have clear policies on dealing with bullying and cyberbullying, please contact the schools or view our websites for a copy of these policies.

Here are some general points to help deal with Cyberbullying:

- If you feel you are being bullied by email, text or online, do talk to someone you trust.
- Never send any bullying or threatening messages.
- Keep and save any bullying email, text or images.
- If you can make a note of the time and date bullying messages or images were sent and note any details about the sender.
- Use blocking software; you can block instant messages from certain people, “unfriend” people on social networking sites or use mail filters to block email.
- **Do not** reply to bullying or threatening messages or emails; this could make matters worse. It also lets the bullying people know that they have found a “live” number, email address or “active” social networking contact.
- **Do not** give out your personal details online; if you are in a chatroom, online game or IM session watch what you say about where you live, the school you go to, your email address, your friends and family. All these things can help someone build up a picture about you.
- **Do not** forward abusive texts, email or images to anyone. You could be breaking the law just by forwarding them. If they are about you, keep them as evidence.
- **Do not ever** give out passwords!
- **Remember** that sending abusive or threatening messages is against the law.
- **Do** report instances of cyberbullying you have seen or heard about, even if not directed at you. There is no such thing as an innocent bystander, if you have seen the posts, messages or images then you could be considered as part of it if you do not report it!

APPENDIX 1.0

STAFF, GOVERNOR & VOLUNTEERS AUP

OUR VISION

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to all users and in particular children. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe internet access at all times. Lack of guidance and learning in E-safety can mean staff, volunteers and children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate all members of the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience. Our policy and practice against this is clearly articulated in this Acceptable Use Policy.

> ***'Our vision is to make the children at Woodstock School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'***

THIS ACCEPTABLE USE POLICY IS INTENDED TO ENSURE:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the children in my care in the safe use of ICT and embed e-safety in my work with them.

PROFESSIONAL AND PERSONAL SAFETY:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (for example, laptops, email, iPads and other electronic devices) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
  A strong password consists of at least six characters that are a combination of uppercase / lowercase letters, numbers and symbols (@, #, $, %, etc.)

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate people (via the E-Safety Incident Recording Form that is passed to the Headteacher).
- I will report incidents of concern regarding children's safety to the school's designated Child Protection Co-ordinator (Headteacher).
- I will promote E-Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

BEING PROFESSIONAL IN MY COMMUNICATIONS AND ACTIONS WHEN USING SCHOOL ICT SYSTEMS:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website, in weekly newsletter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers via the school office using the official school system
- I will not engage in any on-line activity that may compromise my professional responsibilities.

THE SCHOOL AND THE LOCAL AUTHORITY HAVE THE RESPONSIBILITY TO PROVIDE SAFE AND SECURE ACCESS TO TECHNOLOGIES AND ENSURE THE SMOOTH RUNNING OF THE SCHOOL:

- When I use my mobile devices (laptops, mobile phones, iPads, USB devices) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will **not** use personal email addresses on any school ICT equipment.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with school standard practice.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/ security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings unless agreed by the Headteacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy'. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

WHEN USING THE INTERNET IN MY PROFESSIONAL CAPACITY OR FOR SCHOOL SANCTIONED PERSONAL USE:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright or intellectual property rights, I will respect these and not download or distribute copies (including music and videos).

I UNDERSTAND THAT I AM RESPONSIBLE FOR MY ACTIONS IN AND OUT OF THE SCHOOL:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

ACCEPTABLE USE POLICY (AUP)
Staff, Governor & Volunteer Consent Form

I have read and understood the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I have read and understood the school E-safety Policy and agree to work within the outlined practices.

PERMISSION TO SET UP ACCESS & USE THE INTERNET		
I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure safety during use of the Internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies. I understand that my activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.		
I give permission for a username and password to be set up for me to have access to ICT systems at school and the Internet in accordance with the school's E-safety and Acceptable Use policies	***YES***	***NO***

PERMISSION TO USE DIGITAL IMAGES & VIDEOS		
I agree to the school taking and using digital or video images of me in accordance with the school's GDPR Policy, and understand that the images will only be used to support pupils' learning activities or in publicity that reasonably celebrates success and promotes the work of the school, as follows:		
School notice boards	***YES***	***NO***
Newsletters	***YES***	***NO***
School website	***YES***	***NO***
School's internally-located television	***YES***	***NO***
School projectors & whiteboards	***YES***	***NO***
Local newspapers	***YES***	***NO***
I agree to only take and use digital/video images at, or of, school events, for school use, and not to publish these or make them publicly available on social media.	***YES***	***NO***

In the event that you leave the school, personal information, data and images will not be used by the school in the production of any new communication items listed above.

NAME:	
SIGNED:	
DATE:	

APPENDIX 1.1

Acceptable Use Policy

OUR VISION

Woodstock CE Primary School is committed to safeguarding and promoting the welfare of children. All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to all users and in particular children. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe Internet access at all times. Lack of guidance and learning in E-safety can mean staff, volunteers and children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate all members of the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience. Our policy and practice against this is clearly articulated in this Acceptable Use Policy.

'Our vision is to make the children at Woodstock School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'

THIS ACCEPTABLE USE POLICY IS INTENDED TO ENSURE:

- Children will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of E-safety and are involved in the education and guidance of their children with regard to their on-line behaviour.

The school will ensure that pupils have good access to digital technologies, including educational programmes and games as well as the Internet to enhance their learning and, in return, expects pupils to be responsible users.
The use of digital & video images plays an important part in learning activities. Pupils and members of staff may use school digital cameras or iPads to record evidence of activities in lessons and on trips/visits etc. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. At no time will children have unsupervised access to IT equipment and the Internet.

The school will comply with the General Data Protection Regulations and request parents/carers' permission before taking images of members of the school. We will also ensure that when images are published that the child cannot be identified by the use of their names.
In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (such use is not covered by the

General Data Protection Regulations). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents and carers comment on any activities involving other pupils in the digital/video images.

ACCEPTABLE USE POLICY (Pupils)

Pupils must use ICT systems in a responsible way in and out of school, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users.

This involves:

- Asking a member of staff if they want to use a computer or other equipment.
- Only using their own log-in and password, keeping it safe and secure, and remembering to log-out when they have finished.
- Only using activities that a member of staff has allowed them to use.
- Taking care of the computer and other equipment.
- Asking for help from a member of staff if they are not sure what to do or if they think something isn't right.
- Telling a member of staff if they see something that they are unhappy with or which upsets them on the screen.
- Understanding that the school may check or monitor how they use digital technology.
- Knowing that if they break the rules they might not be allowed to use a computer or other equipment.
- Understanding the risks and not trying to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- Not trying to use any programs or software that might allow pupils to bypass the filtering/security systems in place to prevent access to such materials.
- Immediately reporting any damage or faults involving equipment or software, however this may have happened.
- Not accessing any emails in school.
- Not installing or attempting to install, or store programs of any type on any school device, nor trying to alter computer settings.
- Not bringing own computer, mobile devices, memory sticks or personal storage devices into school without permission from the class teacher.
- Understand that pupils are not permitted or able to access or use social media sites within school.
- Ensuring that pupils have obtained permission to use the original work of others in their own work.
- Where work is protected by copyright, not trying to download copies (including music and videos).
- When using the Internet to find information, taking care to check that the information accessed is accurate, as the work of others may not be factual and could be misleading or an attempt to influence opinions.
- Respecting others' work and property and not accessing, copying, removing or otherwise altering any other users' files, without the owner's knowledge and permission.
- Being polite and responsible when communicating with others, and not using strong, aggressive or inappropriate language. Appreciating that others may have different opinions.
- Not taking or distributing images of anyone without their permission.

THIS POLICY OPERATES ON THE UNDERSTANDING THAT PUPILS RECOGNISE THAT:

- The school may check or monitor how they have used the computer.
- That the school also has the right to take action against pupils if they are involved in incidents of inappropriate behaviour, that are covered in this agreement, when they are out of school and where they involve membership of the school community (examples would be cyber-bullying, use of images or personal information).
- If they were to break this Acceptable Use Policy Agreement, there would be consequences to their actions. This may include removal of Internet or computer access, contact with parents and in the event of illegal activities involvement of the police.

ACCEPTABLE USE POLICY (AUP)
Parent Consent Form

CHILD'S NAME: | **YEAR GROUP:**

PERMISSION TO SET UP ACCESS & USE THE INTERNET		
I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies. I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's E-safety.		
I give permission for a username and password to be set up for my child to have access to ICT systems at school and the Internet in accordance with the school's E-safety and Acceptable Use policies	***YES***	***NO***

PERMISSION TO USE DIGITAL IMAGES & VIDEOS		
I agree to the school taking and using digital or video images of my child in accordance with the school's GDPR Policy, and understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school, as follows:		
School notice boards	***YES***	***NO***
Newsletters	***YES***	***NO***
School website	***YES***	***NO***
School's internally-located television	***YES***	***NO***
School projectors & whiteboards	***YES***	***NO***
Local newspapers	***YES***	***NO***
I agree to only take and use digital/video images at, or of, school events, which include images of children other than my own, for personal use, and not to publish these or make them publicly available on social media.	***YES***	***NO***

All parents are being asked to re-sign our AUP in line with the General Data Protection Regulations (GDPR) 2018. Once a child leaves our school, personal information, data and images will not be used by the school in the production of any new communication items listed above. This permission will apply throughout the time your child attends Woodstock CE Primary School unless there are significant changes to our Acceptable Use Policy in which case further consent from you will be sought.

SIGNED PARENT:

DATE:

APPENDIX 1.2

E-SAFETY CONTACTS AND REFERENCES

Childnet International
http://www.childnet.com/resources

Childline
http://www.childline.org.uk

Think U Know (links to CEOP)
www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Stop it now (child sexual abuse prevention campaign, for all adults)
www.stopitnow.org.uk

Parents Protect
www.parentsprotect.co.uk

E-Safety self-review tools provided by South West Grid for Learning
www.360safe.org.uk for schools and www.onlinecompass.org.uk for youth settings

Securus (Company supplying software to protect pupils from cyberbullying in schools)
www.securus-software.com

Internet Watch Foundation (IWF)
www.iwf.org.uk was set up by the UK internet industry to provide the UK internet 'Hotline' for the public to report potentially illegal online content.

CBBC Stay Safe
www.bbc.co.uk/cbbc/topics/stay-safe

Web Cam fact sheet
http://www.thinkuknow.co.uk/Documents/Webcam%20fact%20sheet%202.pdf

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta

http://www.becta.org.uk/schools/esafety

e-Safety in Schools
http://www.kenttrustweb.org.uk?esafety

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Safety Zone
http://www.internetsafetyzone.com/ Kent Primary Advisory e-Safety Pages
http://www.kented.org.uk/ngfl/ict/safety.htm

Kidsmart
http://www.kidsmart.org.uk/ NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209 NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy
http://www.eiskent.co.uk (broadband link) Stop Text Bully
www.stoptextbully.com

Report it:

Thames Valley Police – for suspected criminal activity
http://www.thamesvalley.police.uk/reptcr/reptcr-repform.htm

Oxfordshire County Council website – for child safeguarding concern
http://www.oxfordshire.gov.uk/cms/public-site/child-social-care

CEOP – report a child in danger of abuse. Children can self-report.
http://www.ceop.police.uk/safety-centre/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

Internet Watch Foundation – report child sexual abuse content http://www.iwf.org.uk/

Professionals Online Safety Helpline – 0844 3814772 helpline@saferinternet.org.uk

APPENDIX 1.3

Woodstock CE Primary School E-Safety Charter

Safe

- I will only use the Internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the Internet my home address, telephone number or my school's name.
- I will never give my password to anyone, even my best friend, and I will log-off when I have finished using the computer.
- I will never send anyone my picture without permission from my teacher/parent.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I understand that I can only access sites and materials relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material or hack into the school's systems.
- I know that my teacher and the Internet provider will check the sites I have visited.

Meet

- I will never arrange to meet anyone in person.
- I understand that the people I communicate with online may not be who they say they are.

Accepting

- I may not download software from the Internet (including screen savers, games, *.exe files etc.).
- I may only download video clips and audio clips with the permission of a teacher and only then from a directed website and for educational purposes only.

Reliable

- I know I cannot trust everything that I see or read on the Internet.
- I know that information on the Internet may not always be reliable and sources may need checking.
- I have the responsibility to provide information that is not misleading, to keep my own data safe and not to misuse any information I have about others.
- I have the responsibility to check any information before using it.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.

Tell

- I will never respond to unpleasant, suggestive or bullying e-mails and I will always report it to a teacher/parent.
- If someone says or writes something, not just on the computer but also through texts, which makes me feel uncomfortable or worries I will always report it to a teacher/parent.
- I will not look for bad language or distasteful images while I'm online and I will report these to a teacher/parent if I come across them accidentally.

I promise to always be **SMART** when using the internet.

SHARED WITH CHILDREN BY THE CLASS TEACHER & E-SAFETY REP

PLEASE SIGN YOUR AGREEMENT BELOW

CLASS:_____

APPENDIX 1.4

CLASS TEACHER INTERNET SAFETY CHECK

It is good practice to discuss these points with pupils at the start of the school year, the start of a project requiring Internet use, or if revision of Acceptable Internet Use is necessary.

- ✓ Only use the Internet when there is a teacher or other adult present to supervise or when you have been given specific permission.
- ✓ Only use your own login name and password. Never use another person's details.
- ✓ Never give out your address, phone number or arrange to meet someone over the Internet.
- ✓ All e-mails, messages in forums and text messages should be polite, appropriate and sensible. Do not send any e-mail or text message which could cause upset.
- ✓ If you receive a rude or offensive message you must report it to a teacher immediately. Do not pass on rude or offensive messages. What may seem funny to you may not be funny to someone else.
- ✓ If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher or to an appropriate member of staff.
- ✓ Be aware that the school may check your computer files and monitor the Internet sites you visit.
- ✓ Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate.
- ✓ You and your parents should have signed the school Internet Agreement. You will be breaking that Agreement if you deliberately break these rules. This could result in you losing your Internet access at school.

Draw pupil's attention to the poster on the wall in the classroom regarding sensible conduct whilst using the Internet. They can refer to this anytime they need a reminder.

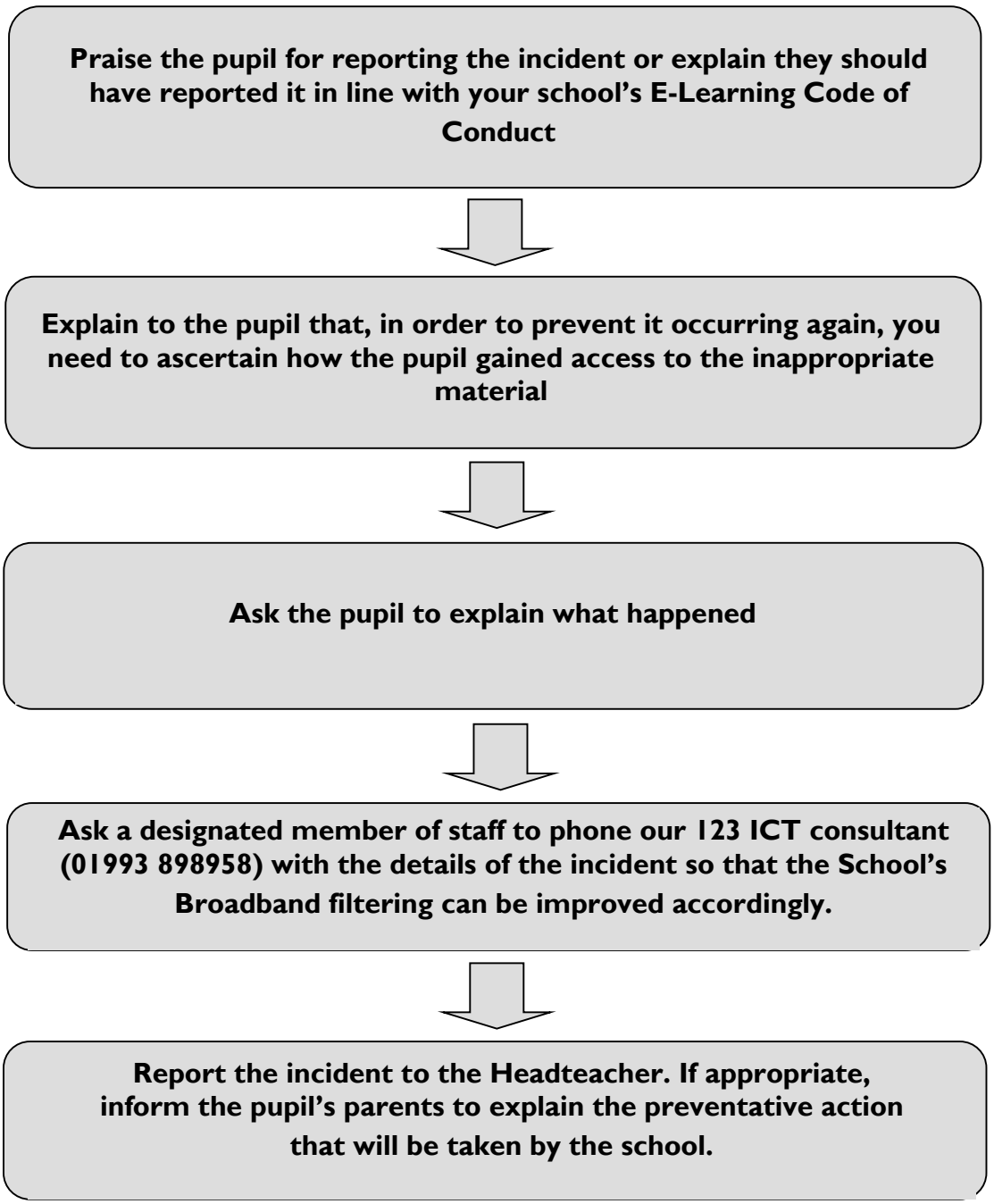
woodstock
CE PRIMARY SCHOOL

APPENDIX 1.5

GUIDELINES ON INAPPROPRIATE INTERNET ACCESS

Whilst using the Internet during school hours, a pupil **accidentally** finds a website displaying inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for reporting inappropriate materials from the Internet.



E-SAFETY INCIDENT RECORDING FORM

APPENDIX 1.6

Please record sufficient detail to enable the monitoring of incidents.

Type of Incident:	✓	**System Location:**	✓
Bullying (cyber bullying)		Library	
Grooming		Classroom	
Sharing inappropriate messages		Corridor	
Sending inappropriate images		Outside school premises	
Hacking or virus spreading		Other (record in **description** below)	
Accessing racist, sexual or homophobic material			
Sharing racist, sexual or homophobic material		**Device accessed on:**	✓
Accessing religious hate material		Laptop	
Sharing religious hate material		Desktop computer	
Accessing pornographic material		iPad/Tablet	
Sharing pornographic material		Mobile phone	
Other (record in **description** below)		Other (record in **description** below)	

Date:	**Time:**
Description of what happened:	

Accidental Access:	**Deliberate Access:**

Child/ren Involved:	Year	SEN	Disability	Ethnic Group	Involvement in Incident

Member of staff recording the incident:
Role:

Other staff involved:
Role:

Action Taken:		
If appropriate:	Yes ✓	No ✓
Have you copied Incident Form for class teacher?		
Have you had contact with the parents/carers of all children involved? If Yes, by phone / letter? Date of contact:		
Are any other agencies involved? If Yes, which agencies? If Yes, and the incident was prejudice-motivated, consult Local Authority as to whether a Hate Crime report is appropriate.		
Does the incident require Police/CEOP involvement?		

Signed:

Name:

Date:

Status:	✓
Resolved	
Unresolved	
Further intervention needed	
123 ICT informed (if appropriate)	

File THREE Copies (tick when actioned)	**Headteacher**	**Child's File**	**E-safety File**
Details of any subsequent actions or follow-up: (Include dates)			