- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead and the E-Safety Coordinator
- The Headteacher should be aware of the procedures to be follo

- Online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, and can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties, including jail
- How information and data is generated, collected, shared and used online
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

Students should be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use both within, and outside, school. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Staff should act as good role models in their use of digital technologies, the Internet and mobile devices at all times.

5.1 Educating Parents about online safety

Many parents and carers have only a limited understanding of online safety risks and issues, yet play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to raise parents' awareness of internet safety in letters home as well as the school newsletter and in information via the schools website, Facebook page and Twitter feed. Parents can also access the schools Safeguarding webpage and E-Safety Guidance where they can access links to other support and information such as: www.swgfl.org.uk , http://www.saferinternet.org.uk/ , http://www.childnet.com/parents-and-carers

This policy may also be shared with parents. Online safety may also be covered during parents' evenings.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils on a regular basis, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying where appropriate to their subject.

All staff (including support staff), governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying as part of the school newsletter to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL and E-safety Coordinator will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on student's electronic devices, including mobile phones, tablets and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine, or erase data or files, on an electronic device, staff must involve the DSL as well as a technician, and reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm
- Disrupt teaching
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material
- Retain it as evidence (of a criminal offence or a breach of school discipline)
- Report it to the police

Any searching of students will be carried out in line with the DofE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the School Complaints Procedure.

7. Acceptable use of the Internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (Appendices 1, 2 and 3). Visitors will be expected to read and agree to the school's terms on acceptable use when relevant.

Use of the school's Internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor, and filter, the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Staff may choose to apply for unfiltered access, if needed, and will therefore sign the unfiltered AUP. However this is still monitored and has filters for certain areas.

More information is set out for

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can rec

Appendix 1: Acceptable Use Policy (Student)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I am aware that technology is changing, and using AI may help me with my work, but I am honest and will only use AI if it has been agreed with my teacher. I will acknowledge where, and how, I have used AI. I know exam boards have rules on the use of AI, which the teacher will explain, and I will keep to these rules. I am aware that my grade may be in question if I misuse this technology.
- When using my own personal social media accounts I must ensure all posts relating to school / school activities are presented positively and respectfully in line with school expectations and I understand that if I fail to do this then sanctions may be put in

Appendix 2: Acceptable Use Policy (Staff)

Haygrove School Staff Acceptable Use Policy Agreement (Network and Computer Devices)

This Acceptable Use Policy is intended to ensure:

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

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

I recognise and respect the value of the use of technology for enhancing learning.

New technologies / devices have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

I will seek permission from the schools e-safety co-ordinator first before setting up any school related social media, and then share school-related social media account details with IT technicians in order for them to check

Appendix 3: Staff Unfiltered Access Policy

Haygrove School – Acceptable Use Policy – Staff Unfiltered Internet Service

By signing this form you accept and fully understand that any breach of this acceptable use policy can result in disciplinary action by the school and / or the police

Once approved access to the Unfiltered Internet Service will be available through any teaching PC, office PC, admin PC and staff quiet room.

REMEMBER: Unfiltered Access will display any pop-ups, adverts or images that would otherwise have been filtered so please be careful when searching online. There is still some filtering in place and you will still be monitored.

If a student contacts you with regards to problems they are experiencing with social networking, you must not try to deal with this yourself using your Unfiltered Access. You MUST report this to the Designated Safeguarding Leader or the E-Safety Coordinator.

I will at all times comply with the Staff Acceptable Use Policy, for which I will have signed in order to be authorised to use the Unfiltered Internet Service. If at any point this Acceptable Use Policy is broken, I will lose access to the Unfiltered Internet Service.

I will ensure that when using Unfiltered Internet Service, I do not display materials that are inappropriate through my whiteboard, or otherwise.

I will at no point use the Unfiltered Internet Service in any way that may bring the school into disrepute or may harm my professional standing. As part of this I will ensure all materials used have been checked and are appropriate for the educational purpose intended.

I will refrain from "streaming" large video files or using streaming audio sites that could slow down the school network. I will personally check all videos before showing to students, including any adverts or comments if from an online platform to check for appropriateness.

I will not download and install any software at any point for any reason without contacting the Network Manager (Stephen Hudd).

I am aware that the Unfiltered Internet Service is provided to me solely for the purpose of aiding effective teaching and learning and not for me to use socially i.e. for personal social media - facebook / twitter etc.

I must continue to use only the designated email service (Microsoft Exchange – County Email). I am not permitted to use hotmail or any other third party email service for any professional communications.

I am aware that extreme breaches of this Acceptable Use Policy are electronically reported to the County Council and the police. Haygrove School has no control over this.

If at any point, I see or access material accidentally that I feel is inappropriate I must stop what I am doing and report it immediately to the ICT office.

I will not allow students to use my PC at any point for any purpose.

I will ensure that my PC is locked at all times when I am not using it. I must always close my browser when I have finished using the unfiltered network and must not allow anyone else to use the service through my connection.

I confirm that I have read, understood and agreed with the Unfiltered Internet Service Acceptable Use Policy. If at any point I am concerned that an action I may take could breach the Acceptable Use Policy in any way then Don't Do It. Check It.

I also confirm that I have received a formal briefing by the E-Safety Coordinator prior to receiving my access to the Unfiltered Internet Service.

Name (Printed): _____

Signed: _____

Date:_____/_____/_____

Briefing received by E-Safety Coordinator: YES / NO

Signature of E-Safety Coordinator: _____ Date: _____/_____/_____

Appendix 5

Use of video streaming e.g. Youtube

Appendix 5ii: Monitoring and Reporting Incidents (Staff)

Staff	Possible Actions					Possible Sanctions		
Incidents:	Refer to line manager	Refer to myconfide	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action

Appendix 1: Acceptable Use Policy Extension (Technician/Administrator)

The school ICT Technician or person with administration rights is placed in an exceptional position of trust. Many of the duties that the Headteacher expects these people to complete could be against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows ICT Staff to fulfil these duties.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage

- Be careful to make sure that they are observed whenarueful 16M9westhoseri(ed s)11(urv)62(eful)4(1cid)15ymake

Be cT0.000008866 0 594.96 842.04 reW* nBT/F2 11.04 Tf1 0 0 1 74.664 7848512 m671 00 G[Be)-46(cs)11(f)0153()-eT-154 Staf7(o)