HAYGROVE SCHOOL

E-Safety Policy

LINKS: Health and Safety Policy, Data Protection Policy, Child Protection and Safeguarding Policy, Behaviour Policy, Staff disciplinary Procedures, School Complaints Procedure.

DATE: February 2019

POSTHOLDER RESPONSIBLE: K Whitlock - E-Safety Coordinator

DATE RATIFIED BY STANDARDS & PERFORMANCE COMMITTEE: May 2019

AUDIENCE: Staff, Students, Parents, Visitors

DATE OF NEXT REVIEW: May 2021 (two year review cycle)

Contents

1. Aims... 3

2. Legislation and guidance 3

3. Roles and responsibilities 3

4. Educating pupils about online safety 6

5. Educating parents and the wider community about online safety 6

6. Cyber-bullying 7

7. Acceptable use of the internet in school 8

8. Pupils using mobile devices in school 8

9. Staff using work devices outside school 8

10. How the school will respond to issues of misuse 8

11. Training 9

12. Monitoring arrangements 9

13. Links with other policies 9

Appendix 1: Acceptable use policy (students) 10

Appendix 2: Acceptable use policy (staff) 13

Appendix 3: Acceptable use policy - unfiltered internet access (staff) 16

Appendix 4: Online safety training needs – self-audit for staff 18

Appendix 5: Online safety incident report log 19

Appendix 6: Monitoring and Reporting Incidents 20

Appendix 7: Haygrove Filtering Change & Firewall Procedure 24

Appendix 8: Technician / Administrator Acceptable Use Policy 25

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring and reviewing this policy and its effectiveness.

All governors will:

- Have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

3.2 The Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

3.3 The Designated Safeguarding Lead and E-Safety Co-ordinator

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding Policy.

The DSL and E-Safety Coordinator take lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher, Senior Leadership Team and Governing board

3.4 The Network Manager and Technical Staff

The Network manager is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider Opendium. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (appendix 2 and 3) These keep pupils safe from potentially harmful and inappropriate content and contact online whilst at school, including terrorist and extremist material. This includes blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware. There will be regular reviews of the safety and security of school technical systems, and that such safety mechanisms are updated regularly.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. This includes conducting a full security check and monitoring the school's ICT systems on a regular basis. The school infrastructure and individual workstations are protected by up-to-date anti-virus software.
- All users will be provided with a username and secure password by the Network Manager or Head of Computing, who will keep an up-to-date record of users and their usernames. Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. All users are responsible for the security of their username and password. The "master / administrator" passwords for the academy ICT system, used by the Network must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- All users will have clearly defined access rights to academy technical systems and devices. Users can be made aware of their own group policy access rights at any time by contacting the IT department, although any changes to these rights is solely at the discretion of the Network Manager/Head of Computing. Any changes must comply with this e-safety policy and the AUP of the requesting individual.
- The school has provided differentiated user-level filtering, allowing different filtering levels for different groups of users – admin staff / teachers / HoD / HoY / students
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers) onto the school systems.
- School technicians regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. LanSchool is used to enable this process both by teachers of computing classes and the IT department.
- An agreed policy is in place in the Acceptable Use Agreement that forbids staff from downloading executable files and installing programmes on school devices. Requests for adding software or applications to devices must be made to the IT department who will carry out the installation. Requests for additional applications are granted at the discretion of the Network manager.
- Removable media (eg memory sticks / CDs / DVDs) by users on school devices are only allowed if they are suitably encrypted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. This includes ensuring that any online safety incidents and/or cyber-bullying are logged and dealt with appropriately in line with this policy (Appendix 6), as well as the behavior policy.

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- The Network Manager is responsible for ensuring that software license logs are accurate and up to date.
- Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

3.5 All staff

All staff, including contractors and agency staff, are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the DSL or E-Safety Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.6 Parents

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, school social media pages and information about national and local e-safety campaigns and literature. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet, including the use of digital and video images taken at school or school events
- Agree to the policy of students use of personal devices in the academy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree and sign the terms on acceptable use.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the Computing curriculum, however the safe use of social media and the internet will also be covered in other subjects where relevant. Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit by using the software provided. Any discovered breaches should be reported to either the E-Safety Coordinator or a member of the technical Staff.

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be in writing in advance, with clear reasons for the need.

The school will regularly use assemblies to raise pupils' awareness of the dangers that can be encountered online. Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial activities

The e-safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities. A planned e-safety curriculum will be provided as part of Computing at KS3 and will be revisited throughout years 10 and 11 in Tutor time or assemblies.

In **Key Stage 3**, pupils will be taught using the framework "Education for a Connected World" produced by UKCCIS: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF This includes:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- 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 Agreement and encouraged to adopt safe and responsible use both within and outside school

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 e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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 webpage on E-Safety 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.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL or E-Safety Coordinator.

5.2 Education – The Wider Community

The academy will provide opportunities for families to gain from the Academy's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide e-safety information for the wider community.
- Providing family learning courses in use of new digital technologies, digital literacy and e-safety.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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. Tutors will also discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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 regular 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, iPads 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 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.

More information is set out in the acceptable use agreements in Appendices 1, 2 and 3.

8. Pupils using mobile devices in school

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. Students may bring mobile devices into school, but are not permitted to use them during:

- Lessons, or between lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Students may only use their mobile devices at break or lunchtime.

Any use of mobile devices in school by students must be in line with their Acceptable Use Policy (see Appendix 1). Any breach of their Acceptable Use Policy by a student will trigger disciplinary action in line with the School Behaviour Policy and will result in the confiscation of their device.

9. Staff using work devices (or personal devices used for work) outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in Appendix 2.

Staff must ensure that the work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. If staff have any concerns over the security of their device, they must seek advice from the technician.

Work devices must be used solely for work activities.

Any USB devices containing data relating to the school must be encrypted.

Any personal device used for work should be password protected, have up-to-date anti-virus / firewall software installed and the member of staff should have a technician review the safety/ security of the device.

10. How the school will respond to issues of misuse

Where a student misuses the school’s ICT systems or internet, we will follow the procedures set out in the behaviour policy and the student’s account may be locked whilst an investigation takes place. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, which will include network use, safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring arrangements

The E-Safety Coordinator and/or the technical staff log behaviour and safeguarding issues related to online safety. An example of the incident report log can be found in appendix 5.

This policy will be reviewed every 2 years by the E-safety Coordinator. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection Policy
- Health and Safety Policy

Appendix 1: Acceptable Use Policy (Students)

STUDENT ACCEPTABLE USE POLICY

Haygrove School has a clear policy when allowing students to access the schools ICT network. This document is designed to keep you safe and is split into different sections:

Personal Benefits

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety nor to the safety and security of the ICT systems and other users.

- I understand that the school will actively monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password securely. I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material, messages or anything that makes me feel uncomfortable when I see it on-line.

Equality

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- 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 use the school ICT systems for online activities that would breach this policy such as online shopping.

How I treat others

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, and when working collaboratively. I will respect all group members' contributions and only edit with permission of the group.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images, videos or recordings of anyone without their permission.

Helping the school

- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I must follow the rules set out in this agreement, in the same way as if I was using school equipment, and only use them to save my own / my groups work.
- I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person / organisation sending the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not run any executables or programs of any type on a machine

Being a responsible citizen

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including images, music and videos).
- 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.
- 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 place by the school in line with the School Behaviour Policy.
- I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images, videos or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to sanctions from the school. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the following sections to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

✂---

Student Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school).
- I use my own equipment in school (when allowed) eg mobile phones, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, school online platforms such as Google Classroom, website etc.

Student Name in full (Please Print):_________________________________ Tutor Group:______

Student Signature: ____

Parents/Carer Signature : ____ Date:___ / ___ /___

Appendix 2: Acceptable Use Policy (Staff)

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

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. 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.

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 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 students 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 students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my 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 (eg laptops, email) out of school, and to the transfer of personal data (digital or paper based) out of school (personal data including academic data and contact information relating to any adult or student a the 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 (outside of school hours) and that recreational use will also be in accordance to the AUP.
- I will not disclose my username or password to anyone else, unless required by an ICT Technician for support, 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. I understand that I have a responsibility to protect my school profile by ensuring my computer equipment is logged off or locked when I am not present. To ensure further protection of my profile I understand that I should change my password on a regular basis.
- I understand that I have a responsibility to immediately report any illegal, inappropriate or harmful material or incident (including incidents under the counter-terrorism and security Act 2015), I become aware of by other staff, students and my own personal use of computer equipment, to the appropriate person.
- When using my personal social media I will not make any reference to students/parents/carers/school staff nor mention the school in any way that could be deemed unprofessional. I will not engage in online discussions on personal matters relating to the school community.

- When using my personal social media I will not upload, or share, images or recordings of students relating to school activities, nor will I communicate with parents/carers on posts about school related matters.
- I will share school-related social media account details with ICT technicians in order for them to check regulations

I will be professional in my communications and actions when using school / academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files. If for any reason I need to access a student's files, then I will ask an ICT technician to do so for me.
- 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 not use my personal equipment or personal social media to record or publish images / videos / sound involving students. 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. Where these images are published (e.g. on the school website, social media) they will follow permissions given to the school by a parent / guardian.
- I will only use chat and social networking sites in school for work purposes and in accordance with the school's policies. I understand that any private social networking sites that I create, edit or contribute to, and any online activity that I engage with inside and outside school, does not compromise my professional role in school (e.g. posting of offensive content, contacting students). I understand that social networks update their terms of service on a regular basis and therefore I need to update my security settings on a regular basis to ensure appropriate privacy settings.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner. I understand that communication must be written in such a way that it cannot be considered to be abusive, defamatory or libellous . I accept all liability for my communications. I must ensure that written statements cannot be construed out of context .
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / Tablet / Mobile phone / USB devices etc.) in school or at home to access the schools cloud/remote computing platform, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. I will also follow any additional rules set by the academy about such use, including encryption. I will log out of the schools' cloud / remote user computing platform when I have finished using it, to prevent un-authorised access.
- I will not use personal email addresses on the academy ICT systems, I will not use my personal Apple account on school owned Apple devices that students may be using.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes.) If I have any concerns about the validity of the e-mail I will check with an IT technician before opening.
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- 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 programmes of any type on any device/PC, or store programmes on a computer, nor will I try to alter computer settings, without consent from the ICT manager.
- I will not disable or cause any damage to school / academy 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 Academy Personal Data Policy. Where I need to transfer digital personal data outside the secure local network, including the use of Portable storage / USB devices or via the email system, it must be encrypted.
- I understand that the Data Protection Policy requires that any staff or student 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 academy 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, in accordance with copyright.
- Where work is protected by copyright, I will not download or distribute copies (including images, music and videos).

I understand that I am responsible for my actions in and out of the academy:

I will report any breach of the above acceptable use policy to the Head of Computing / Network manager and in their absence I will report any breach to my line manager. I will ensure the information I receive regarding children becoming victims of any breach of the students AUP or any incident which compromises their safety online or otherwise is reported to the child protection officer. Equally I will report to a relevant senior leader any incident involving electronic communications, whether from a child or adult, that compromises my safety or professional standing.

I understand that this Acceptable Use Policy applies not only to my work and use of academy ICT equipment in school, but also applies to my use of academy 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 academy

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.

I have read and understand 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.

Staff / Volunteer Name

Signed

Date

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.

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 - Gregg Walters or the E-Safety Coordinator – Kate Whitlock.

- 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 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 <u>Don't Do It. Check It.</u>

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: ______/_________/________

A copy of this signed acceptable use policy is required to be held on record by the ICT department. This will be stored in your personnel file and is accessible via Maxine Collins.

Appendix 4: Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Can you name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are you familiar with the school’s approach to using social media, both personally and professionally?	
Do you know how to use the schools monitoring software when teaching in an ICT suite?	
Do you monitor any use of students’ own devices if they are allowed to use them in your lesson? If so how?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5: Online safety incident report Log Examplar

Online safety incident report log					
Date	Student Name and Year	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 6: Monitoring and Reporting Incidents

The school believes that the activities referred to in the table below would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Not acceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				*	
Using school systems to run a private business, File sharing (using p2p networks such as U Torrent)					*	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					*	
Creating or propagating computer viruses or other harmful files					*	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				*		
On-line gaming (educational)			*			
On-line gaming (non-educational)			*	*		
On-line gambling					*	
On-line shopping / commerce			*			
Use of video broadcasting e.g. Youtube			*			

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow the restrictions set out in this document. However, there may be times when infringements could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The school will follow the policies laid out in the Child protection and Safeguarding Policy and will inform necessary members of staff immediately to ensure the safeguarding of our young people. The School will also report the incident to the police and ensure the preservation of evidence. Illegal activity will be saved in to the ICT Evidence area

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows: Inappropriate activity will be saved in to the Evidence folder on F.

Appendix 6i: Monitoring and Reporting Incidents (Students)

Students	Possible Actions / Sanctions								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers.	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	*	*	*	*	*	*	*		*
Unauthorised use of non-educational sites during lessons	*				*	*			
Unauthorised use of mobile phone / digital camera / other handheld device	*	*							
Unauthorised use of social networking / instant messaging / personal email	*	*			*				
Unauthorised downloading or uploading of files	*	*			*				
Allowing others to access school network by sharing username and passwords	*	*			*				
Attempting to access or accessing the school network, using another student's / pupil's account	*	*			*				
Attempting to access or accessing the school network, using the account of a member of staff	*	*	*		*	*	*	*	*
Corrupting or destroying the data of other users	*	*			*	*	*	*	*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*			*	*	*	*	*
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*	*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*		*	*	*	*	*
Using proxy sites or other means to subvert the school's filtering system	*	*			*	*	*	*	*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*			*	*			
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*	*
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	*	*	*		*	*	*	*	*

Appendix 6ii: Monitoring and Reporting Incidents (Staff)

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		*	*	*			*	*
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	*							
Unauthorised downloading or uploading of files	*				*			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	*		*		*			
Careless use of personal data e.g. holding or transferring data in an insecure manner	*							
Deliberate actions to breach data protection or network security rules	*	*	*		*	*	*	*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	*	*	*					
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*	*					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	*	*						
Actions which could compromise the staff member's professional standing	*	*	*					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*			*	*	*
Using proxy sites or other means to subvert the school's filtering system	*	*	*					
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*	*		*			
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*
Breaching copyright or licensing regulations	*							
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*

Appendix 7: Haygrove Firewall/Filtering Change Procedure

Haygrove Firewall/Filtering Change Procedure

Purpose:

To outline the process for changes/requests including-

- Firewall Ports opening
- Port Forwarding
- Firewall Rules
- Website White or Black listing
- Filtering Categories and Groups
- Filter Overrides
- Permissions and Limits

The firewall/filter is implemented to protect the Schools network from unauthorised use and to protect sensitive data stored on the Schools computer systems.

Procedure:

All firewall changes will be evaluated to ensure they conform to current security best practices and do not conflict with any existing rules in-place. Opendium/Iceni will also advise on changes prior to implementation.

Firewall changes will only be made by the ICT department or by Opendium/Iceni under instructions from the school.

All firewall changes will be logged in the Firewall Change Log on the ICT dept. \Audit folder, the log includes the following information-

- Name of requester
- Source of Traffic (IP/Hostname)
- Destination of Traffic (IP/Hostname)
- Port Number(s) and name of service needed (i.e 25/SMTP)
- Details/Reasons for change
- Date of change

A monthly change Audit log report will be run each month and saved to the ICT dept. \Audit folder

For example:

Fri May 25 11:30:33 2018	SKenney	88.211.101.82	webfront_filtering ▸ category ▸ uri ▸ delete	Deleted URI from category : webcache.googleusercontent.com
Fri May 25 11:18:49 2018	LCapel	88.211.101.82	webfront_webproxy ▸ override_editor ▸ update	Updated metadata for override Staff Whitelist
Fri May 25 11:18:49 2018	LCapel	88.211.101.82	webfront_webproxy ▸ override_editor ▸ uri ▸ update	Updated URI in override Staff Whitelist: eweb01.e-marker.co.uk/:443 -&gt; eweb01.e-marker.co.uk:443

Haygrove School – Administrator/Technician

Acceptable Use Policy Extension

The school ICT Staff or person with administration rights is placed in an exceptional position of trust. Many of the duties that the Head Teacher 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. Schools should customise this document to fit their needs.

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 systems (e.g. USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, extremist, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.

- User accounts will need to be created and serviced meaning that there may be access to these accounts by ICT Staff and the Administrator.

- Through work within the school's administration network ICT Staff may be placed in the position of assisting in the processing of sensitive personal data including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The ICT Staff, through specific user names and passwords, has control (sometimes through remote workstations) to the school's network. In the past there have been examples where these powers have been abused.

  Because of these areas of concern the ICT Staff should:

  - be responsible for monitoring the school's network.
  - be given permission to access other user's files.
  - protect the users by maintaining a filter for the school.
  - monitor the internet use of users within the school.
  - be aware of the laws relating to the use of computers especially those around Data Protection, Prevent and intimate Sexting images, copyright and those referred to in the school's Online Safety Policy and AUPs.

- Make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.

- Have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- Receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information and the school's Prevent duty.

- Have an agreed procedure for managing the internet filter. This should include a log of decisions made and actions taken.

- Have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet

- Have agreed procedures for reporting incidents.

- Log any incidents including minor ones that are quickly resolved.

- Be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise including:
    - secure and switch off any device that is suspected of containing an intimate sexting image and report to safeguarding lead
    - never open websites that are suspected of having inappropriate material unless others are present

- Have frequent meetings with their line manger to report on any issues or trends.

As a member of ICT Staff (or a person who has administration responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

Name: ____

Signed: ____

Senior Member of Staff: ____

Date: ____