HAZELDENE SCHOOL

E-SAFETY AND AUP POLICY
REVIEWED SEPTEMBER 2018

SIGNED …… DATE……..
HEADTEACHER

SIGNED …… DATE …….
CHAIR OF GOVERNORS

TO BE REVIEWED JAN 2020

Hazeldene School

Contents

……

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 this policy and holding the headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governor who oversees online safety is Stuart Bolton

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy.
The DSL takes lead responsibility for online safety in school, in particular:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT Leader, E Safety Leader, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including supply staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

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 (appendix 1)

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 to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

All pupils will be taught five basic rules for internet safety at home and school including

1. Safe – stay safe, keep your personal information safe
2. Meet – meeting can be dangerous, never meet someone you've met online
3. Accept – only accept emails, messages, files, calls etc from people you know and trust
4. Reliable – not everything you see on the internet is true, not everyone you talk to is reliable or trust worthy
5. Tell – tell an adult if something makes you uncomfortable online

In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer materials that are appropriate to the age range and ability of the group being taught. The class teacher will provide appropriate guidance to pupils as they make use of the internet to conduct research and other studies. All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

While pupils may be able to move beyond those resources which have been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Before conducting research, teachers will carry out appropriate checks

on key words and internet websites, before pupil use. The schools internet access is controlled by accredited filtering software, which should stop access to many inappropriate sites, although we recognise that no system is totally secure. The ICT and E-safety leaders will carry out regular, supervised, checks to ensure filtering software is appropriate and up to date.

The children are aware that if inappropriate sites, images or words are accidentally accessed they should turn the monitor off and then report immediately to their class teacher. Through the use of 'think u know' materials in E-Safety lessons the children are also aware of the CEOP button, and how to use this, should a situation arise.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website
This policy will also be shared with parents.
Online safety will 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 headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as 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, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their children, 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. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying 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 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.

Pupils are responsible for good behaviour on the internet just as they are in a classroom or a school corridor. General rules apply.

The internet is provided for pupils to conduct staff guided research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.
Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the values the school holds.
School may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks will always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following will not be tolerated:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing or insulting others
- Damaging computers, computer systems or computer networks
- Violating copyright laws by downloading copyrighted items
- Using others' passwords
- Trespassing in others' folders, work or files

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 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if 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.
More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils in years 5 and 6 may bring mobile devices into school, but are not permitted to use them during:

Lessons

Clubs before or after school, or any other activities organised by the school

All mobile phones must be handed into the teacher in the morning

9. Staff using work devices 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 their 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. Any USB devices containing data relating to the school must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. 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, on 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 and deputies 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.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL/E Safety Lead logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.
This policy will be reviewed every 2 years

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- GDPR policy and privacy notices
- Complaints procedure
- Data Breach Policy

Acceptable Use Policy

The requirement to ensure that pupils, staff and, indeed, all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. This framework of e-safety, or acceptable use policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place as well as other existing policies in respect of its employees.

Given the glittering array of new technologies now available to use for educational purposes and in everyday life, the intention of this evolving policy is:

- To maximise e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use

As such, the school more specifically intends:

- To provide a secure network for the school and secure means of home/school access
- To monitor traffic, log incidents and act accordingly
- To establish key standards and behaviour for e-safety across the school, in keeping with those of the Local Authority
- To co-ordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines and acceptable use policies for pupils, staff, parents and governors
- To ensure that we adhere to e-safety issues related to new government policies affecting schools
- To monitor the school's responses to e-safety matters and act accordingly
- At Hazeldene the persons responsible for E Safety are Mrs Ward the DSL, Mrs J Chapman, liaising with Miss E Moulder, ICT leader

E-safety is a whole-school issue, not something that is simply the responsibility of the ICT Leader. As such, the whole school has a responsibility to promote it.

Guidelines

The AUP aims to:

- Reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.
- Enable young people to develop their own protection strategies when adult supervision and technological protection are not available.
- Provide information on where to seek help and how to report incidents
- Help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines and information for parents, carers and others on safe practice.
- Ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Strategy

This policy is the result of ideas discussed by the school community. The policy has been put to the school staff and ratified by the Governors. Parents are informed through the School Booklet, guidelines distributed during Parents' Evenings and the pupils' AUP which is signed by them and their children at the beginning of the school year. E-Safety guidelines are displayed in the computer areas.

Passwords
Staff and pupil passwords are kept private and only the holder can change them. It is accepted that from time to time, e.g. forgetting a password, the ICT manager can help to create a new password but s/he will not know what it is. Computers must not be left in 'logged on' mode. As it is good practice users will change their passwords monthly.

Emails
All staff are provided with their own personal login and email address via the It's Learning platform. This email address should be used for all school correspondence. It is accepted that staff may send emails and attachments to recipients outside the school. When doing so emails should refer to initials of children only, personal information about children should not be shared via email. Children may only send emails under the supervision and direction of their teacher.

Anti-virus and anti-spam system

The school has an up to date anti-virus and also an anti-spam system provided by the Local Authority which is updated weekly. The network is set up to automatically scan laptops and other portable devices every time they are connected to the school system.

Video Conferencing

Under the direct supervision of a teacher/TA children may participate in video-conferencing with other schools.

Restricted (Named staff only)	Protected (All in school community)	Public (Anyone)
Any information that identifies an individual	Routines, management information	Website, display

Access to all ICT systems shall be via logins and passwords.

Inappropriate content and language
There will be zero tolerance to the use of inappropriate content and language on any ICT equipment within our school community.

The type of language that is used in emails should be no different to that which is used in face to face situations.

Staff and Visitors

The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to e-safety during staff training sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies. Working at this school means acceptance of those policies including this AUP.

As such:
Staff must use the It's Learning email account for school related matters, eg. Planning

Staff must not allow any emails between themselves and pupils to be anything other than school business.Staff must not have any pupil (or former pupils) as 'on line' friends if they are of school age (under 16 years of age). Staff must report to the Head Teacher any contact from a pupil or former pupil of school age.

Staff should not make reference to any child, parent or the school on social networking sites such as Facebook.

Staff should have mobiles switched off during lesson times.

During ICT lessons pupils should be made aware of the procedures for reporting accidental access to inappropriate materials. In any instance of deliberate misuse the E Safety Leader must be informed and the pupil will be dealt with in accordance with the school's behaviour policy.

The school email accounts may be used for personal use.

Staff should keep to a minimum any data which is held on their school laptop and they must lock it if it is left unattended (ctrl + alt + delete, lock).
The security of school laptops out of school lies with the staff who, by taking them off school premises, accept responsibility for them.

PCs for pupils must be arranged in classrooms to allow good teacher supervision.

All photographs containing children must be stored on the school network by the ICT manager who will arrange for the deletion of them within three years of the child leaving unless parental permission has been given to retain them longer e.g. for publicity purposes). Children's full names will not be posted online or in an out of school context.

All online accounts created for children and staff should be deleted within two weeks of leaving the school.

Any restricted data that is taken away from the school premises must be securely encrypted on school devices and only accessed on those devices. Restricted data must be backed up by the Network Manager on a drive specifically set up for this purpose.

Exporting SIMS data must only be on school devices.

Pupils

ICT Code of Conduct
will be referred to in the School Handbook and will be placed on the School Website. The children's ICT Code of Conduct will be displayed on the E-Safety display board and around computer work stations. Pupils should be reminded of internet safety rules when using the Internet.

When using the internet children will be taught;

- how to critically evaluate materials
- good searching skills
- the importance of intellectual property regarding materials they find on the internet

Pupils are involved, through the School Council and the work done in ICT lessons in which activities to promote good practice and internet safety issues are delivered, in the evolution of this AUP and the following guidance:

Pupils are not encouraged to bring in to school personally owned devices unless they have been so requested by their teacher. Any such device should be handed into the school office for safekeeping until such time as they are required or collected at the end of the school day.

Pupils learn about the good practice that is appropriate for social networking through the use of the blogging facility on the school network to which they are introduced during ICT lessons.
Pupils are made aware of the procedures for reporting accidental access to inappropriate materials.

If children accidentally find inappropriate material they are to report it to their teacher who will alert the E Safety Leader so that s/he can take steps to rectify this. Staff who find inappropriate material will report it directly to the E Safety Leader Children learn of this procedure in their lessons and it is reinforced. Staff are made aware of their responsibilities in this during staff training and by having their own copy of the policy.

Sanctions
Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school by the E Safety Leader,

School Website

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. The school will obtain parental permission before using images of pupils on the website. We ensure the image file is appropriately named. This reduces the risk of inappropriate, unsolicited attention from people outside school. Images will be appropriately stored and secured on the school's network.

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: Use them for a non-educational purpose Use them without a teacher being present, or without a teacher's permission Access any inappropriate websites Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) Use any inappropriate language when communicating online, including in emails Share my password with others or log in to the school's network using someone else's details Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: I will not use it during lessons or other activities organised by the school and I will hand it in to my teacher in the morning I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open 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 will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• That the schools' 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 will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff 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 the young people 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.

Safety for my professional and personal use:

• 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 (e.g. laptops, email, tablets, etc.) 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 will immediately report any illegal, inappropriate or harmful material or incident, I

become aware of, to a member of the Senior Leadership team.

I will be 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 only use my personal equipment to record these images if it is password protected.

• I will only use chat and social networking sites in school in accordance with the school's policies.

• I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.

• I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.

• If the data on any device is breached I will report it to the Senior Leadership Team

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

• When I use my personal hand held / external devices (iPads/PDAs / laptops / mobile phones / USB devices etc.) 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 open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

• I understand the importance of regularly backing up my work.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, 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 a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

• 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 personal data is transferred outside the secure school network, it must be encrypted.

• I understand that the data protection policy requires that any staff or young person's 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

• It is my responsibility to understand and comply with current copyright legislation.
I understand that I am responsible for my actions in and out of 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 out of school, and my use of personal equipment in school 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 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.

Signed (staff member/governor/volunteer/visitor)	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil 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 there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

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

Appendix five Code of conduct for children

Always ask an adult
Only use the Internet with adult permission.

Supervision
Never use a computer without an adult present in the room.

Never give anyone your personal details.
Never give any information which would help anyone work out where you live or who you are. You would not give your name and address to a stranger you meet at a bus stop. So do not give your full name, telephone number or address when working on the Internet. The same applies about giving information about your family and friends.

Do not to arrange to meet people through the Internet.
Remember, not everyone you 'meet' on-line are who they say they are. People can pretend to be someone else.

Do not look for things on the internet that are rude, racist or illegal. Don't reply to bad messages.
If you come across things that are deliberately rude, racist, illegal or things that make you feel uncomfortable tell an adult, who will inform our service provider.

Ask 'Is it True'
Just because it comes out of a computer does not mean it is true! Some people make up things. Always check where the information has come from and check it.

Never delete, change or read other people's e-mails, files or passwords.
We share our network so remember to be careful. You do not want your work deleted or changed, so don't do it to others. Never attempt to log on as somebody else.

Do not play computer games that are not suitable for school.
If you are playing games, make sure they are in line with the schools Code of Conduct – we don't have fighting in school, so don't play games that involve fighting. Don't play games which are violent or are meant for older children or adults.

Do not download or listen to music.
If music is free to download then it is usually illegal. Don't listen to music in school that is rude, racist or is meant for older children or adults.

Remember! The whole world is watching.
Do not write things that would upset or offend other people. Others will judge you, your school and your family, by what they see on the screen.

Appendix six what to do if you see something that concerns you

It is likely that at some point you will come across some images or words that you did not intend to see. If this happens and you do see or hear something that scares, worries or upsets you do the following immediately.

- Turn the computer screen off! Do not turn the PC off.

- Put your hand up and ask for a teacher to come straight over.
- DO NOT show other pupils what you have seen or discuss with them.
- Wait for someone to come over and help you quietly.

The Teacher will then tell you what to do next.