HAZELDENE SCHOOL

E-SAFETY/AUP POLICY

REVIEWED OCTOBER 2017

SIGNED …… DATE……..
HEADTEACHER

SIGNED …… DATE …….
CHAIR OF GOVERNORS

TO BE REVIEWED OCTOBER 2019

E-SAFETY/AUP POLICY

Rationale

The school encourages use by pupils of the rich information and interactive resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills are fundamental in the society to which our pupils belong.

On-line services open classrooms to a broad array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the pupils. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by pupils.

Electronic information research skills are fundamental to the preparation of citizens and future employees. The school expects that staff will investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the appropriate use of such resources. Staff will consult the ICT Leader for advice on content, training and appropriate teaching levels.

Access to on-line resources will enable pupils to explore thousands of libraries, databases, and activities while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media, information and gaming sources. To that end, the school supports and respects each family's right to decide whether or not to allow pupils internet access within the school environment.

School Procedures

Resource Development

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.
The staff are aware that all inappropriate sites accidentally accessed in school should be reported to the E-Safety leader – Mrs J Chapman, who will then liaise the ICT leader, Head teacher and ICT technician.

School Rules
The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to all pupils, and kept under constant review. All pupils, parents/carers are to sign an internet code of conduct, and agree to the terms of the acceptable usage policy.

All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

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

Pupil Guidelines for Internet Use

General

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

Sanctions

Violations of the above rules will result in a temporary or permanent ban on computer and internet use in school.

Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

Hazeldene School Pupil Acceptable Use Agreement / E Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E Safety.

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Miss Moulder/Mrs Chapman ICT/E-safety Leaders.

✂---

Parent/ carer signature

We have discussed this and ……………………………………..........(child name) agrees to follow the E-Safety rules and to support the safe use of ICT at Hazeldene School.

Parent/ Carer Signature …………………………………………………….

Class …………………………………. Date ………………………………

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
- To have a named Senior Information Risk Officer – (SIRO) – to co-ordinate the development and implementation of e-safety policies, with clear designated responsibilities, and liaise with the Local Authority in such matters. At Hazeldene Lower the persons responsible are 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. It is good practice for users to change their passwords regularly.

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, parentmail, display

Access to all ICT systems shall be via logins and passwords. Any exception must be SIRO approved. All information storage shall be restricted to necessary users with any additional access being SIRO approved. The SIRO must maintain a record of who has access to restricted information.

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.

Inappropriate Web content:

Chat rooms/instant messenging (except that promoted by the school for educational purposes)	Newsgroups/forums (except that promoted by the school for educational purposes
Downloads of ring tones, screensavers and games (except any promoted by the school for educational purposes)	Internet peer to peer networks
Downloads of freeware, shareware, evaluation packages (except by authorised persons and in compliance with copyright law)	Online gaming sites which link to an online community (except any that have been sanctioned by the school for educational purposes)

The SIRO will maintain an incident log and report on its use once a year to the governing body.

Date of Incident	Description	Immediate corrective action	Further action	Legal Implications	

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 SIRO 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 SIRO 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 need to be aware that conducting any personal transactions could result in residual information remaining on the hard drive which may be accessible to others. **Neither the school nor the Local Authority can accept any liability for any resulting loss or damage.**

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 two 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 (see appendix 2) 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.
The school cannot accept any responsibility for personally owned devices (e.g. laptops, USB devices, external hard drives, mobile phones and digital cameras) brought into school or taken on educational visits. If these are to be used on the school network they must, on a daily basis, first be virus checked before they are connected or used. They can only be taken on educational visits at the discretion of the teacher in charge and provided that pupils agree to use them appropriately as they would in school.
School data should not be stored on these devices other than for the time it is actually being used.
The VLE should be used as the means for accessing such data off school premises.
The school accepts the use of school email addresses by pupils in other schools providing they adhere to the pupil AUP.

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 SIRO so that s/he can take steps to rectify this. Staff who find inappropriate material will report it directly to the SIRO. 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 SIRO,

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.

OCTOBER 2017

This policy will be reviewed every 2 years

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 Two 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.