



HALE CE

PRIMARY SCHOOL

E-safety Policy

Hear of the Community

Acepting everyone

Love of God and neighbour

Excellence for all

Reviewed: May 2020

Adopted by GB at Summer Term Meeting -

E-SAFETY POLICY

Responsibilities

The member of school responsible for e-safety is Caroline Millington.

They are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the college community. He/she may also be required to deliver workshops for parents.

Internet use and Acceptable Use Policies (AUPs)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role.

Examples of the AUPS used can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip.

This can be found in appendix 2

AUP's will be reviewed annually. All AUPs will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff need to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection Act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

Hale CE Primary School recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.

The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

Hale CE Primary School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in the classrooms or in the play areas during school time. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. If staff need to make an emergency call, they must do so either in the staff room or main or Headteacher's office. Staff must ensure that there is no inappropriate or illegal content on the device.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Members of staff may only contact a parent/carer on school approved mobile phones. Pupils should not use mobile phones within the school grounds. Mobile phones should be handed in at the start of the day and collected at the end.

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises. If they wish to make or take an emergency call they may use either the staff room or the main office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

Important contact details are kept on the school's mobile phone in case of an emergency.

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers/practitioners or volunteers at the school understand the difference between appropriate and inappropriate sharing of images.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails

Pupils should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to be used in school.

Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the office. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to Caroline Millington.in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, ChildLine).

Infringements and sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Level 1 infringements:-

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone

Level 2 infringements:-

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Unauthorised use of mobile phone (or other new technologies)
- Continued use of unauthorised instant messaging / social networking sites
- Use of File sharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent

Level 3 infringements:-

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents.

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.
- Bringing the school name into disrepute

Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer.

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – e.g. class commendation for good research skills, certificates for being good cyber citizens etc. Each year group teacher will indicate these opportunities within the provided planning.

Social networking

Pupils are not permitted to use social networking sites within school.

E-Safety Education Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

- a). A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- b). Regular auditing, review and revision of the computing curriculum
- c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
- d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc.

Additionally,

- a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- c). The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour
- d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

- a). A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
- b). E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
- c). All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
- d). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
- e). Staff are encouraged to undertake additional e-safety training such as CEOP training
- f). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
- g). The school takes every opportunity to research and understand good practice that is taking place in other schools
- h). Governors are offered the opportunity to undertake training.

Parents and the wider community

The school provides e-safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety co-ordinator.

Monitoring and reporting

- a). The school network provides a level of filtering and monitoring that supports safeguarding.

b). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

c). The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Halton Local Authority (where necessary)
- Halton Safeguarding Children Board

d). The school action plan indicates any planned action based on the above.

Acceptable Use Policy for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - inappropriate images
 - promoting discrimination of any kind
 - promoting violence or bullying
 - promoting racial or religious hatred
 - promoting illegal acts
 - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs etc. that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____ Print name _____ Date _____

ACCEPTABLE USE POLICY: EYFS

To help me stay safe on a computer or iPad

- I will only use a computer or iPad when an adult tells me I can.
- I will ask for help if I think I have made a mistake or I am stuck.
- I will be careful when using a computer, iPad or Beebot.
- I will tell an adult if I see something on the computer that makes me unhappy.

ACCEPTABLE USE POLICY: KS1

To help me stay safe on a computer or iPad ...

- I will keep passwords safe and not share them
- I will take care of the computer, iPad and other computing equipment
- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use websites, apps and programmes that a teacher or suitable adult has told or allowed me to use
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will press the minimise button and tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I do not follow the rules then I may not be able to use the computer or iPad

I understand that if I do not follow the rules then I may not be able to use the computer or iPad.

Signed _____

Date _____

ACCEPTABLE USE POLICY: KS2

To help me stay safe on a computer or iPad ...

Personal safety

- I will keep my password safe and will not use anyone else's (even with their permission).
- I will never share my personal details, such as my full name or address, with people I don't know.
- I will not use a personal mobile device in school unless I have been given permission by an adult in school
- I will only give my mobile phone number to friends I know in real life and trust
- I understand that my use of the internet will be monitored
- I will always tell an adult if something on the Internet makes me or my friends unhappy.
- I will minimise the screen if something appears that makes me feel unhappy so my teacher can look into it.
- I will ask permission before using the Internet and use it for a specific purpose
- I will never meet up with someone I have met on the Internet.
- I know I should not believe everything I read on the Internet.
- I am aware of the CEOP report button and know when to use it

Safety of others

- I will be polite and responsible when I communicate with others
- I will always check my messages are polite before I send them.
- I will not reply to a message that isn't kind, but I will save it and show it to an adult.
- I will not share images of anyone without their permission
- I will not share personal information of other people I know
- I will not take photographs or video in my school uniform

Safety of the school

- I will not open or download a file unless I have been given permission by an adult in school
- I will not try and access anything that is illegal
- I will not edit or remove files on the computer system
- I will not download apps or install updates on an iPad
- I will tell a responsible adult if I damage or there are any faults with technology, however this may have happened.

I understand that if I do not follow the rules then I may not be able to use the computer or iPad.

Signed _____

Date _____

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

Hale CE Primary School

Parent / guardian name:.....

Pupil name:

Pupil's registration class:

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent / Guardians' signature:.....

Your name (in block capitals):

Date:.....

Appendix 3 – School audit

Audit

The self-audit in should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Halton guidance? Yes

Date of latest update (at least annual): June 2020.....

The Leadership team member responsible for e-safety is: Caroline Millington.....

The governor responsible for e-Safety is: ...Mike Fry.....

The designated member of staff for child protection is: Marianne Mowatt.....

The e-Safety Coordinator is: Becky Ford.....

The e-Safety Policy was approved by the Governors on June 18.....

The policy is available for staff at: School website and policy file

The policy is available for parents/carers at: School website

Date of E-safety training for staffMarch 2017 and ongoing.....

Date of Prevent trainingSeptember 2019.....

Appendix 4 – Photo/video consent

School Name:

Name of pupil:

Class:

During the year the staff may take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.

To comply with Data Protection Regulations, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please return the completed form to school. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

1. May we use your child’s image in our printed promotional publications? Yes / No
2. May we use your child’s image on the school website/SLG? Yes / No
3. May we record your child’s image on our promotional videos? Yes / No
4. May we use your child’s image in the local press? Yes / No

Signature:

Your name (in block capitals).....

Date: