Halsall St Cuthbert's C.E. Primary School

E-Safety Policy

Equal Opportunities

At Halsall St Cuthbert's Primary School we recognise the responsibility of all schools to provide a broad and balanced curriculum for all pupils. All children should have equal access to resources and activities enabling them to develop their skills to the best of their personal ability. The SENCo and ICT Co-ordinator jointly advise teachers on the support which can be provided for individual children with particular educational needs, including high ability pupils. Specialist equipment will be purchased as required to meet specific needs.

Document Purpose

E-Safety at Halsall St Cuthbert's CE Primary school is a priority and whilst we want to encourage the pupils to use a diverse selection of modern technology to further their progress and enjoyment we have a duty to ensure that the children use technology in a safe manner.

Many of the aspects of E-safety fall outside school's parameters however, it is essential that the children in our care are given the tools they need to use advancing technology safely. Maximising opportunities is a fundamental element in Halsall St Cuthbert's Mission Statement, technology is key to progress and enjoyment and, at Halsall, we want to maximise the benefits and opportunities ICT has to offer.

The children's learning environment must be secure; hence, we equip the pupils with the skills and knowledge to use not only the technology available in school but the technology that is widely available to children outside school, appropriately and responsibly. We feel it vital to work with parents and carers in their roles in encourage the safe use of technology.

E-Safety Leadership

At Halsall St Cuthbert's we acknowledge the importance of school representatives from the school community. The e-Safety Leader will be a point of contact for e-Safety related issues.

Designated e-Safety Leader: Miss Kate Hampson

The role of the e-Safety Leader should include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's e-Safety Policy and associated documents, including Acceptable Use Policies.

- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an e-Safety incident occur.
- Ensuring an e-Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with e-Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging e-Safety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person/Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

Security and data management

At Halsall St Cuthbert's, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Secure data is available to staff at the discretion of the Head Teacher.
- Staff are permitted to use removable devices such as: pen drives and cameras. Staff are asked to be vigilant when using such devices remotely and must not take any confidential data outside of the school building.
- Confidential data is stored only on the secure staff network. It cannot be accessed without passwords which are known only to the teaching staff.
- Data is backed up daily on the Office system and staff network to ensure data is not lost.

Use of mobile devices

At Halsall St Cuthbert's, we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

Mobile phones

- Staff are allowed to bring personal mobile phones into school. They must ensure the device is password protected.
- Staff are permitted to bring their phones into the classroom but they must be on 'silent' and may not be accessed during lesson time unless special

permission has been granted by the Head Teacher. See child protection policy section 13.
- Pupils are not permitted to bring mobile phones to school unless special arrangements have been made. In these cases the mobile phone will be kept in the school office or with the class teacher.

IPads
- iPads must remain in school at all times unless permission is given by Head Teacher/ICT Co-Ordinator
- iPads must be returned to the secure storage when not in use.
- Images and videos taken using the iPads should only be downloaded to the school server.
- The ICT coordinator and class teachers will have overall control of downloaded apps.
- Staff will not be permitted to use their own account to download apps.
- All pupils will be made aware of the acceptable use policy and understand the sanctions of misuse.

Laptops
- Staff laptops can be taken home.
- Staff are aware of the responsibility they have to ensure all content on these devices is legal and appropriate for a school setting.
- All laptops will be password protected and staff made aware of the importance of changing passwords on a regular basis.

Use of digital media (cameras and recording devices)

At Halsall St Cuthbert's we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.
- Only children with parental consent may appear in media pertaining to the school – newspaper articles/photos, website articles/photos, newsletters.
- Parental consent is requested by all parents on admission to the school. The wishes of those parents who choose not to consent are adhered to. (See Appendix 1)
- School may retain images of past pupils on the Website until such a time that it is updated.
- Full names and personal details will not be used in conjunction with any digital media, particularly in association with photographs.
- Parents and carers are not permitted to take photos/videos of their children in school (for example in assemblies, sports days etc.)

- Parents are asked not to publish any photos taken during school events on social networking sites as they may not have the permission of the parents of the pupils in the image. See consent form.
- Pupils are not permitted to publish any school related images of themselves or other pupils on social networking sites.
- Staff are not permitted to publish any school related photos on social networking sites.
- Staff must only use the school camera/iPad to take photographs of the children. These devices must not be taken home.

Communication technologies - Email

At Halsall St Cuthbert's the following statements reflect our practice in the use of email:

- It is recommended that all staff have access to the Lancashire Grid for Learning e-mail service. This is the preferred school e-mail system.
- Only official school e-mail addresses should be used to contact staff.
- The risk of SPAM is enormous when using external e-mail accounts, SPAM can often contain unsuitable material and viruses, and therefore, children are not permitted to access their external e-mail accounts in school.
- Staff are asked to be vigilant when accessing external e-mail accounts in school and should do so only when essential.
- Staff are reminded that it is essential to use safe practice when sending data via e-mail from school. E-mails are covered by the Data Protection Act.
- Pupils may be given a group email account. This account must not contain any information that could identify the identity of a pupil.

Social Networks

At Halsall St Cuthbert's the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- School uses the BT Firewall hence, social networking sites are blocked on all school computers, other than those with designated responsibility for updating school accounts.
- Children are encouraged to follow the rules of the social networking site – particularly age restrictions for membership.
- All members of staff are given regular training on acceptable use.
- Pupils using social networking sites are reminded of the safe use and are not permitted to use any school photos on their site.
- Staff should not accept pupils or ex pupils (of school age) as their 'friends'. They are encouraged not to accept parents as 'friends'.

- Staff are not permitted to engage in any discussion, via social networking, regarding school matters.

School Website

At Halsall St Cuthbert's the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- All staff are made aware of the safe publication of media on the school website.
- All staff are aware of the guidance regarding personal information on the school website.
- The Head Teacher, ICT Technician and the staff have access to edit the school website.
- Any downloadable documents available on the school's website (Newsletters) will be available in 'read only' format, to prevent the content being manipulated.
- The school website contains a link to e-Safety websites and to the relevant policy documents.

Infrastructure and technology

As Halsall St Cuthbert's subscribes to Lancashire Grid for Learning and CLEO Broadband, the internet content available to staff and pupils is filtered by default. It is important to note that this filtering service offers a high level of protection. Sophos Anti-Virus is also used on all school computers and regular updates are received.

Pupil's Access

All pupils are permitted access to the internet and through e-Safety lesson are taught how to use this safely and appropriately. Any inappropriate use will result in appropriate sanctions being taken. Pupils can only access certain areas of the network.

Adult Access

Staff will login to access secure areas of the school network.

Software/hardware

School has legal ownership of all hardware and software. Licenses are kept in a secure place. The ICT Co-ordinator audits the software and equipment. The ICT Technician controls the installation of the software onto the server.

Managing the network and technical support

At Halsall St Cuthbert's we are aware that a safe network is required to ensure staff and pupils can work effectively. In order to ensure can happen the following procedures are used:

- The server, the wireless system, the hub and the cabling are all restricted.
- The ICT technician has access to all the above.
- All wireless devices are security enabled.
- The ICT Technician is responsible for the managing the school network system.
- Staff are asked to log out of their system once they have finished.
- The ICT Technician ensure that security of the server is kept up to date.
- Pupils are not permitted to bring pen drives into school, unless given permission by ICT co-ordinator.
- Staff cannot access the school network remotely.
- If staff use their laptop at home they are aware of appropriate use and dangers of infections being brought into school.
- The subject leader liaises with the ICT Technician on a weekly basis.

Filtering and virus protection

- Halsall St Cuthbert's use the LGFL and CLEO Broadband filtering system.
- All staff are aware of the procedures for reporting suspected or actual virus infection.

Dealing with incidents

The Head Teacher and E-Safety Leader will monitor all recorded offences. Any incidents regarding E-Safety must be logged and a record completed. Any suspected illegal offences should be brought to the attention of the Head Teacher immediately. It is important that any incidents of inappropriate use of technology are dealt with quickly. The school must decide on appropriate sanctions.

Inappropriate use

At Halsall St Cuthbert's we aim to ensure all staff and pupils can work in a safe environment and are aware that on occasions rules may be broken. The following procedures and sanctions are used to address any incidents of misuse:

Accidental access to inappropriate materials:

- Minimise the webpage/turn the monitor off
- Tell a trusted adult.
- Enter the details in the Incident Log and report to LGfL filtering services if necessary.
- Persistent 'accidental' offenders may need further disciplinary action.

Using other people's logins and passwords maliciously.

- Inform SLT or designated e-Safety Leader.
- Enter the details in the Incident Log.
- Additional awareness raising of e-Safety issues and the AUP with individual child/class.
- More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
- Consider parent/carer involvement.

Deliberate searching for inappropriate materials:

- Inform SLT or designated e-Safety Leader.
- Enter the details in the Incident Log.
- Inform parent/carer involvement.
- Remove ICT privileges for an agreed period.

Bringing inappropriate electronic files from home:

- Inform SLT or designated e-Safety Leader.
- Enter the details in the Incident Log.
- Inform parent/carer of the incident
- Contact appropriate services if more serious.

Acceptable Use Policy (AUP)

Staff and pupils are asked to sign an AUP. Pupils are asked to sign when they reach KS2 and staff are asked to sign when they commence work at Halsall St Cuthbert's. The children and staff are reminded of the AUP annually. The AUP is displayed in each classroom (See Appendix 2, 3 and 4)

Education and training

At Halsall St Cuthbert's we are aware that adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, we realise it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. The three main areas of e-Safety risk (as mentioned by OFSTED, 2013) that we make our pupils and staff aware of and consider are:

Content:

- Children need to be taught that not all content is appropriate or from a reliable source.
- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example proanorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact:

- Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.
- Grooming
- Cyber bullying in all forms
- Identity theft and sharing passwords.

Conduct:

- Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.
- Privacy issues, including disclosure of personal information, digital footprint and online reputation
- Health and well-being - amount of time spent online (internet or gaming).
- Sexting (sending and receiving of personally intimate images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film). (Ofsted, 2013, Inspecting e-Safety – guidance document)

e-Safety - Across the curriculum

In the 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential

that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

- E-Safety is taught from the Foundation Stage to Year 6 during lessons, assemblies, PSHE using approved resources from CEOP and NSPCC.
- E-Safety will be differentiated through support for pupils with SEN.
- Pupils are reminded annually of the AUP and their own responsibility to act safely both inside and outside school.

e-Safety – Raising staff awareness

- Staff will receive INSET training and staff meeting training on E-Safety.
- Staff are asked to sign an AUP regarding social networking and are advised of the impact social networking can have on their personal safety and professional conduct.
- New staff are asked to sign the AUP and are trained, if needed, by the E-Safety Leader.
- Updates at staff meetings on E-Safety and AUP are held when necessary.

e-Safety – Raising parents/carers awareness

“Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.” (Byron Report, 2008).

- E-Safety will be addressed to parents via the School’s website.
- Parents will be pointed in the direction of E-Safety resources and online materials via the website.
- Parents will be updated on e-Safety matters within school

e-Safety – Raising Governors’ awareness

- Governors will be invited to attend any E-Safety meetings/evenings/INSET
- The E-Safety Policy will be reviewed regularly and approved by the governing body.
- E-Safety will be discussed during curriculum committee meetings.

Evaluating the impact of the e-Safety Policy

At Halsall St Cuthbert’s we recognise the importance of monitoring the impact of safeguarding procedures throughout school. In order to ensure the impact is positive and continuous the following procedures will be followed:

- Incidents will be analysed by the SLT to see if there is a recurring pattern.

- Policy and AUP will be amended if new devices are deemed to pose a risk.
- Governors and staff will be informed of any updates to the policy.

APPENDIX 1

ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will be an active participant in e-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
- I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chatrooms.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I will ensure that all electronic communications with children and other adults are appropriate.
- I will not use the school system(s) for personal use during working hours.
- I will not install any hardware or software without the prior permission of the Senior Leadership Team.
- I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
- I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

- I will report any known misuses of technology, including the unacceptable behaviours of others.
- I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in anyway, using any technology, is unacceptable.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
- I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's e-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……..…….…….

Date…….……..

Full
Name……..……(PRINT)

Position/Role……

APPENDIX 2

ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use any external device to access the school's network e.g. pen drive.
- I will respect copyright and intellectual property rights.
- I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……..…….……

Date…….……

Full
Name……..……(PRINT)

Position/Role……

APPENDIX 3

ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's e-Safety Policy.

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- 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.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

APPENDIX 4

Classroom e-Safety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe with ICT

- We only use the Internet when a trusted adult is with us.
- We are always polite and friendly when using online tools.
- We always make careful choices when we use the Internet.
- We always ask a trusted adult if we need help using the Internet.
- We always tell a trusted adult if we find something that upsets us.

APPENDIX 5

Classroom e-Safety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

- We always ask permission before using the internet.
- We only use the Internet when a trusted adult is around.
- We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).
- We always tell an adult if we see anything we are uncomfortable with.
- We only communicate online with people a trusted adult has approved.
- All our online communications are polite and friendly.
- We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.
- We only use programmes and content which have been installed by the school.

Version 3 **Adoption** July 2018

Review Date Summer 2020

Senior Member of Staff Responsible Doug Scholes

Designated Member of Staff Kate Hampson

Governor Responsible Rev Paul Robinson