Computing and eSafety Policy

"Including all learners and achieving great things"

September 2016

Article 17: Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.

Article 36: Governments must protect children from all other forms of exploitation, for example the exploitation of children for political activities, by the media or for medical research.

Policy Contents

Aims of using Computing in school

The use of ICT in the school is underpinned by the desire to equip our students with the skills, knowledge and understanding to participate in a rapidly changing world in which ICT is already playing a vital role in teaching, learning, leisure and the workplace.

At Halley, our aim is that:

- Computing is presented as a creative and fascinating process in which children are encouraged to use their own initiative, imagination, reasoning and investigative skills across all three areas of Computing: IT, Computing and Digital Literacy
- Computing is integrated across the curriculum, particularly within topic learning, to enhance the chance of meeting the greatest possible range of learning styles in each lesson through resources that offer visual, audio and kinaesthetic stimuli and to allow greater interactivity to increase pupil engagement and motivation
- Children appreciate the relevance of Computing in our society and that they see it as an essential tool for learning, communication, finding information and for controlling and understanding their environment

Computing Curriculum

Computing is taught at Halley as a discrete subject. This enables children to be taught specific skills that will enable them to prosper in an ever-changing world.

At Halley our aim is that:

- Children receive equal opportunity to develop their computing capability, with computing being planned for in line with its status as a core National Curriculum subject
- Children learn to work individually and collaboratively
- Children have a right to learn Computing through different means of technology and software

Organization for Teaching and Learning

<u>Using Computers and iPads</u>

At Halley, we have an ICT suite and set of iPads, all of which are available to children have access to at least once a week. All teaching staff are allocated their own iPads for teaching and assessment use only.

It is of paramount importance that teachers and other adults in the school are aware of, and children are taught, the basic skills of using a computer as well as general rules of conduct when working with others on a laptop; i.e. logging on/off, saving/retrieving files, allowing the computer to carry out a command, treating equipment respectfully.

Children as well as adults sign a user agreement, outlining appropriate use of laptops and general ICT equipment (later in this document).
Children must only use the login and password they have been given by the teacher to access the computer system. Children are not allowed to access other children's files and make changes.

Children are not allowed to bring in CDs and other multi-media resources from outside school and use them on the school computers unless this has been agreed with their teacher. Many of these skills and rules need to be revisited and/or reinforced regularly**.**

In order to keep the computers running safely, food and drink must not be consumed whilst using a computer/laptop.

PPA/Hotdesk room

There is a separate PPA room to be used by teachers for planning, preparation and assessment which is equipped with PCs. The purpose of this room is to allow teachers to have a space whereby they can carry out their additional professional duties. Children are not permitted to use this room. There are also additional desktop computers in the staff room that can be used by support staff and visiting teachers.

Mobile Phones

Adults using mobile phones within school do so at their own risk. Terms of appropriate usage are outlined in the 'Handheld Device and Mobile Phone Policy' later on in this document. If a mobile phone is used to take a photo of a child/ren, then the photo should be removed at the nearest possible opportunity.
On the rare occasion that a child needs to bring a mobile phone to school, parents must ensure that it is given in at the office before school starts and collected at the end of the day.

E-safety

Children are taught and staff sign a user agreement at the start of the year and the terms of appropriate use are discussed before any access is granted to use ICT. The rules of e-safety must be regularly revisited throughout the school year. Resources to teach this are provided by the CEOP (Child Exploitation and Online Protection centre) and the LGfL (London Grid for Learning).

Halley also aims to meet the following E-Safety standards:

- Staff are advised to report any safety/safeguarding issues immediately to any of the e-safety officers
- E-Safety must be taught within every Computing lesson
- CPD sessions for staff and parents/carers must be carried out regularly

Roles and Responsibilities

We all have a duty to enforce E-Safety around school and demonstrate safe use of Computing equipment around school. The contacts below are responsible for certain aspects of Computing within school should you require more information.

Business Manager – Lisa Payne

- To ensure the Computing policy is disseminated and implemented to all staff
- To be aware of any problems/issues likely to impact negatively on standards of attainment
- To be aware of any problems/issues likely to impact negatively on the quality teaching and learning
- To use information gained from school monitoring to identify INSET and professional development needs
- Provide support for software issues across the curriculum and advise accordingly
- Liaise with Network Manager on software purchases
- To work with the SLT and other subject coordinators to develop the use of Computing across the curriculum
- Work with the SLT to develop out of hours access to Computing for students, other adults in the school and the wider community

Computing teacher – (Turn IT On) – one day per week support

- To teach/team teach the Computing curriculum from Reception to Year 6
- To update the termly and yearly curriculum plans
- To provide teaching resources where relevant
- To work with the teachers in class to develop the skills required to teach the curriculum
- Teach alternating classes every term (3 classes per half term)
- To encourage teachers to complete assessment on a regular basis

Network Manager - Michael Donovan (Turn IT On)

- Provide technical support for hardware across curriculum and admin machines
- Manage and maintain schoolservers
- Liaise with SMT and Business Manager on hardware/software purchases
- Maintain a software inventory of PCs across the network
- Check the TIO Support Portal for issues and respond within a reasonable time frame

E-Safety Officers (Helen C – lead, Wendy, Mumina, Samina, Katherine and Kiasha)

- Acting as a named point of contact on all online safety issues and liaising with other membersof staff as appropriate
- Keeping up-to-date with current research, legislation and trends. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda
- Ensuring that the setting participates in local and national events to promote positive online behaviour, e.g. Safer Internet Day
- Ensuring that online safety is promoted to parents and carers and the wider communitythrough a variety of channels and approaches.
- Work with the setting lead for data protection and data security to ensure that practice is in linewith legislation
- Maintaining an online safety incident/action log to record incidents and actions taken as part ofthe schools safeguarding recording structures and mechanisms.
- To monitor the delivery and impact of the online safety policy
- To monitor log of reported online safety incidents to inform future areas of teaching/learning/training
- Monitoring and reporting on online safety issues to the school management team, GoverningBody and other agencies as appropriate
- Liaising with the local authority and other local and national bodies as appropriate

Managing Equipment Policy

This policy outlines general guidance on using the school network, equipment and data safely. The computer system/network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely, the Senior Leadership Team and the School Business Manager:

- Ensures staff read and sign that they have understood the school's Computing and E-Safety Policy and Acceptable User Policy. Following this, they are set up with Internet and email access and can be given an individual network/email login username and password
- Provides pupils with an individual network login username from Year 3 when they are also expected to use a personal password
- Makes it clear that staff must keep their logon details private
- Makes clear that pupils should never be allowed to logon or use teacher and staff logins
- Makes clear that no one should log on as another user
- Has set-up the network with a shared work area for pupils and one for staff
- Requires all users to always log off when they have finished working or lock their computers if they are leaving the computer unattended
- If a user finds a loggedon machine, they must always logoff and then logon again as themselves
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed
- Has setup the network so that users cannot download executable file/programs
- Has blocked access to music download or shopping sites – except those approved for educational purposes
- Maintains equipment to ensure Health and Safety is followed, e.g. projector filters cleaned by Network Manager, equipment installed and checked by approved Suppliers/LA electrical engineers
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems, e.g. technical support or SIMS Support
- Uses our broadband network for our CCTV system and this has been set up by approved LGfL partners
- Uses the LGFL USO FX website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or the DfE
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Reviews the school ICT systems regularly with regard to security

Acceptable Use Policies (AUP)

All adults in school must read the relevant AUP terms and sign two copies of the document. They must retain one copy for their own records and the other will be filed with school records. Full Acceptable Use Policies can be found on the school website. Children are taught about acceptable use.

AUP terms for adults working in school

<u>Use of Mobile Equipment</u>

- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems. I will do this by returning any 'loaned item back to the school premises fortnightly, making sure the item is switched on and updated before removing from site again.
- I will not use personal devices for any storage, editing or transferal of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school using school-approved equipment.
- I will follow the school's policy on use of mobile phones / devices at school and will not take into classrooms / only use in staff areas.
- I agree and accept that iPads or any other equipment loaned to me by the school, is provided solely to support my professional responsibilities and it will be used in accordance of the iPad Acceptable use area of

this document. I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

LGFL, Email, Intranet, School Network and Data

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality policy.
- I will not connect a computer, laptop or other device (including USB flash drive) to the network that does not have up-to-date anti-virus software.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location
- I will use the school's Learning Platform (DB Primary) in accordance with school and LGFL advice.
- I will only use the LGFL system I have access to in accordance with their policies.
- I will only use the approved secure email system (LGFL Mail); school MLE (DB Primary) or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will not reveal my network password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I request for it to be changed by the Network Administrator (Michael Donovan). I will not use anyone else's password if they reveal it to me and will advise them to change it.

Internet and Online Activity

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not browse, download or send material that could be considered offensive by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact/IT technician.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role and do not bring the reputation of the school, its pupils or my colleagues into disrepute
- I will only access school resources remotely (such as from home) using the LGfL/school approved system and follow e-security protocols to interact with them.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.

E-Safety

- I will alert one of the child protection officers (Wendy, Helen, Kiasha, Mumina and Katherine) / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to senior member of staff / designated Child Protection lead.
- I will embed the school's curriculum into my teaching.

AUP terms for EYFS

Halley Primary School

EYFS Acceptable Use Policy

Staying safe whilst using the computer

To help me stay safe on the computer...

I will only use a computer when an adult tells me I can.

I will tell an adult if I see something on the computer that makes me unhappy.

AUP terms for Key Stage 1

Halley Primary School
Including all learners and achieving great things

KS1 Acceptable Use Policy

Staying safe whilst using the computer

To help me stay safe on the computer...

I will only use a computer when an adult tells me I can.

I will keep my password safe and not share it with anyone.

I will always send polite messages.

I will tell an adult if I see something on the computer that makes me unhappy.

AUP terms for Key Stage 2

Halley Primary School

KS2 Acceptable Use Policy

Staying safe whilst using the computer

To help me stay safe on the computer...

I will ask permission before using the Internet and use it for a specific purpose.

I will never share my personal details, such as my full name or address, with people I don't know.

I will never share my password with anyone.

I will never meet up with someone I have met on the Internet.

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 open or download a file unless I am sure it is safe.

I know I should not believe everything I read on the Internet.

I will always tell an adult if something on the Internet makes me or my friends unhappy.

Handheld Device and Mobile Phone Policy

This policy sets out what is 'acceptable' and 'unacceptable' use of mobile phone and handheld devices by the whole school community (pupils, staff and visitors) while they are at school or undertaking school activities away from school.

This applies to all individuals who have access to personal and/or work-related handheld devices within the broadest context of the setting. It includes children and young people, parents and carers, practitioners, volunteers, students, governors, visitors, contractors and community users. This list is not exhaustive.

It is to be recognised that it is the enhanced functions of many handheld devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying.

It must be understood that should handheld devices be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones and handheld devices can also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others.

The purpose of this policy is to prevent unacceptable use of mobile phones, camera-phones and other hand held devices by the school community, and thereby to protect the School's staff and students from undesirable materials, filming, intimidation or harassment.

General issues

- Designated 'mobile use free' areas are situated across the setting, and signs to this effect are displayed throughout. The areas which should be considered most vulnerable include: toilets, classrooms and changing areas.
- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- All visitors to the school are requested to keep their phones on silent.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. Staff should store their devices in personal lockers and use them only in designated break times unless prior permission has been given by the Headteacher.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing areas and toilets. They should only be used in classrooms when pupils are not present.
- The Bluetooth and sharing functions of a device should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Staff use of personal devices

- Staff handheld devices, including mobile phones, tablet devices and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff handheld devices including mobile phones, tablet devices and may be added to the school wireless connection as part of Acceptable Use Agreement.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth and other communication systems should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods.
- Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropboxetc).
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they should hide (by inputting 141) their own mobile number for confidentiality purposes.

Parental use of personal devices

- Parents are requested not to use any mobile devices within the school building unless approval has been granted.
- When attending assemblies and other special events parents are requested, through the display of an information slide, to ensure the private and responsible use of any images or films they have taken of their children.

Use of Digital and Video Images Policy

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website (Headteacher, School Business Manager and Finance and Admin Officer).

Use of still and moving images

Most importantly, take care when using photographs or video footage of pupils on the school website. Consider using group photographs rather than photos of individual children. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

- If the pupil is named, avoid using their photograph / video footage.
- If the photograph /video is used, avoid naming the pupil.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film

If showcasing examples of pupils work consider using only their first names, rather than their full names.

Only use images of pupils in suitable dress to reduce the risk of inappropriate use.
In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken.
Images of pupils whose parents have not given consent during their admission interview will not be published on the school website.

Procedures

Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. All links are checked regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils should always be reviewed before publishing it on the school website. The work will not include the full name of the pupil, or reveal other personal information, such as membership of after school

clubs or any other details that could potentially identify them. Pupils' work should not contain any statements that could be deemed defamatory.

The school will not infringe copyright or intellectual property rights through any content published on the website. (eg using images sourced through Google, or using a Trademark for which copyright permission has not been sought.)

When showcasing school-made digital video work, pupils are not referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Digital images - photographs and video clips - can now readily be taken using mobile phones. Halley staff are advised not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Technical

Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.

When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names.

When using video as part of Halley Visual Literacy work it is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.

If necessary Halley school will use safe online environments for publishing, such as the LGfL portal or Learning Platform and School 'Book Publishing' websites.

Education

Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

Policy statements in this school

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the Headteacher, School Business Manager, Finance and Admin Officer, Network Manager and all class teachers in their class areas on DB Primary
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;

- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal on DB Primary in school;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are taught about how images can be abused in their eSafety education programme;

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although sometimes advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, Facebook, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Policy statements:

- The schools will filter access to most social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.