

# Caroline Haslett Primary School & Faraday Club



## DIGITAL TECHNOLOGIES POLICY

**Date of Issue:** December 2020  
**Date of next review:** December 2022 (or earlier in the event of legislation changes)

**Approved by the Headteacher on:**

**Signed:** \_\_\_\_\_ (Headteacher) **Date:** \_\_\_\_\_

**Approved by the Governing Board on:**

**Signed:** \_\_\_\_\_ (Chair of Governors) **Date:** \_\_\_\_\_

This policy should be read in conjunction with other school policies including Behaviour for Learning (where there is also a relevant Anti-Bullying section), Child Protection, Data Protection and Freedom of Information policies.

## Introduction

This policy aims to cover the different elements that Computing, Information Communication Technology (ICT) and Digital Citizenship can cover within our school. Computing refers to the discrete subject as outlined in the National Curriculum. ICT refers to the cross-curricular uses of ICT resources across the curriculum to enhance learning. Digital Citizenship refers to how to be safe, respectful and responsible when using technology.

These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum. This policy will set out a framework for how Computing, ICT and Digital Citizenship will be taught, assessed and monitored throughout the school and should reflect the ethos and philosophy of our school. This policy has been written with guidance and support from other teachers, schools and local authorities and aims to meet the criteria established by organisations such as 360Safe and Naace. Often schools will have a number of policies including Online safety and Social Media, but as a school we have decided to combine them into one policy. Further information on the different systems in school will be made available to staff throughout meetings and on the shared drive.

## Aims/Rationale

Computing encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent and independent users and learners of Computing, ICT and Digital Citizenship we aim:

- To use Computing resources, where appropriate, to ensure pupils are motivated and inspired in all areas of the curriculum
- To use Computing resources to help improve standards in all subjects across the curriculum
- To develop the Computing competence and skills of pupils through all curriculum lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of Computing across the curriculum and are provided with exciting, creative ways in which to share their learning
- To use Computing resources available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation

## DIGITAL TECHNOLOGIES POLICY

Date of Issue: December 2020

- To provide all staff with the training and support to ensure that they can, and have the confidence to, use Computing resources to their full potential in all aspects of school life
- To use Computing resources as a form of communication with parents, pupils and the wider community
- To support children with their online safety education

### Curriculum

At Caroline Haslett Primary School we teach in three discrete strands: Computing, ICT and Digital Citizenship.

Computing will be taught discreetly and will include a range of pedagogy including “unplugged lessons” which teach concepts without using ICT resources. The Computing topic overviews show learning outcomes for pupils at the end of each Computing strand, for each year group, and allow teachers to plan progressive and challenging Computing lessons for all children. As the Computing curriculum has been recently introduced, teachers will be mindful that prior learning may not be in place and that they may need to refer to younger years’ learning outcomes whilst planning lessons appropriate to the maturity of the pupils. With this in mind, the overview and year group planning will be adapted each year to ensure that it is relevant, up-to-date and challenging.

ICT will be taught across the curriculum and wherever possible, integrated into other subjects. There may be a need for stand-alone ICT objectives to teach skills that can then be used throughout the cross-curricular sessions. Children may be taught ICT using a range of operating systems and devices. The long-term ICT overviews show the outcomes which the children are expected to reach at the end of each phase. These overviews will be adapted each year to ensure that the content is relevant and up-to-date. There will be a selection of age-appropriate websites and tools provided with the overviews and teachers and teaching assistants will be given regular staff meetings to use the ICT resources and ensure they are confident at using them across curriculum.

Digital Citizenship will be taught discreetly on a half termly basis and, wherever possible, integrated into all uses of ICT resources across the curriculum. Children will be taught using a range of online resources that have been recommended in the curriculum overviews. This includes signposts to age-appropriate resources and the expected outcomes for each phase.

The Computing Coordinator will ensure that the overviews provide coverage of what is expected across each of the three strands ensuring these also meet the requirements of the National Curriculum. The Computing Coordinator will ensure that the children are challenged and are able to succeed across a varied and balanced curriculum.

In EYFS, children will be taught how to use various pieces of ICT resources, including tablets, in accordance to the Early Learning Goals appropriate for them. To ensure pupils in the EYFS can be included in whole-school events, such as Computing star of the week, specific activities may be planned.

## Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

On our website, for children in Foundation and Key Stage 1 we will:

- Provide links to generic websites suitable for the age phase (e.g. phonics)
- Provide links to websites suited to the current topic

For Key Stage 2 children, we will also:

- Provide a personal login for our Google Apps environment which will encompass a number of other tools such as photo, audio and website creation

Across the school, we will:

- Provide a 'website of the week' linking parents and children to a range of useful resources

## Assessment

Computing, ICT and Digital Citizenship will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during lessons and will be used to inform future planning; this is conducted by the computing lead teacher on an informal basis. Specific Computing, ICT and Digital Citizenship capability will be completed on a termly basis (HA, MA and LA representative child) with notes being taken by the teacher. This will be combined with samples of the pupil's work to act as evidence for the learning outcomes at that year group.

Following the introduction of the new National Curriculum and the changes to assessment, there are no longer levels of attainment for Computing or ICT. The Computing coordinator has provided a range of learning outcomes for each year group for which children will be assessed on in relation to Computing, ICT and Digital Citizenship. There will be discussion with local primary and secondary schools to ensure that these expectations are consistent with others.

At the end of each unit, children will also complete a self-evaluation form to evaluate their progress and learning. In KS1, pupils will store their work locally on the computers they use or on a year group shared Google Apps login. In KS2, pupils will store their work on individual Google Apps logins.

## Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the ICT resources throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve.

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

Through the use of after school clubs, pupils will have access to the range of ICT resources we have in school and they may use them to provide opportunities for access which may not be available to them in the home.

In the event of remote learning, pupils are given the opportunity to borrow a school device if they do not have access to their own.

### **Roles and Responsibilities - School Governors**

School governors should abide by the guidelines set out for staff and ensure that if they do use the ICT resources within school that they are doing so safely. The school's governors are also responsible for ensuring that our school has an effective, and up-to-date, policy in place. The governing board should review the policy in place of any online safety incidents to review the effectiveness of the management of those situations. The governing board are responsible for nominating a representative to participate in the online safety group ensuring they are up-to-date with emerging risks and threats through technology use. This is the role of the online safety governor.

### **Roles and Responsibilities - Senior Management Team**

The headteacher and other members of the senior management team are responsible for monitoring the teaching of Computing, ICT and Digital Citizenship throughout the school. The senior management team should decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, action plans and timescales. They should also ensure that the Computing coordinator, ICT technician and teachers are following their roles as listed below and in accordance to job specifications and performance management targets. Finally, the senior management team are responsible for ensuring that the members of the online safety group have had appropriate CPD to undertake their day-to-day activities.

### **Roles and Responsibilities - Computing Coordinator**

The Computing Coordinator will oversee planning in all year groups throughout the school and be responsible for raising standards across Computing, ICT and Digital Citizenship. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The Computing Coordinator is responsible for overseeing the assessment of Computing, ICT and Digital Citizenship across the school and providing opportunities to moderate Computing, ICT and Digital Citizenship ability. The Computing Coordinator is responsible for managing equipment and providing guidance for future purchasing in conjunction with the ICT Technician. The Computing coordinator is also responsible for ensuring tools and procedures are sustainable.

### **Roles and Responsibilities - ICT Technician**

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

The ICT technician will oversee the hardware inventory and ensure it is kept up-to-date and ensure the school has the appropriate number, and level, of software licenses for all software. The School Business Manager keeps the list of current licences. The ICT technician is responsible for ensuring all devices have the appropriate software installed and regularly reviews software needs with the Computing Coordinator. They are also responsible for creating user accounts on Google Apps and monitoring the school's email and Internet filters. The ICT technician must ensure that Internet filters are operating correctly at all times. Should a situation occur where internet filters are not working correctly, teachers will be notified straight away all devices will be turned off until the problem is rectified.

The ICT technician is responsible for monitoring that the equipment is stored safely and meets the requirements of the school's insurance provider. The ICT technician is responsible for the day-to-day technological support that may be necessary as and when it occurs. For problems or changes that can be pre-empted, teachers are asked to give at least a week's notice and the ICT technician will deal with it within an appropriate amount of time. If there is any reason the problem cannot be resolved, the ICT technician will liaise with the Computing Coordinator and/or the senior management team to find an alternative solution.

### **Roles and Responsibilities - Online -Safety Group**

The online safety group includes a school governor, a member of the senior management team, the ICT technician, the Computing coordinator and the Digital Leader online safety team. The online safety group will meet on a termly basis. The purpose of the online safety group is to ensure that online safety is regularly thought about and discussed within school. Any incidents that have occurred over the last term are reviewed and any suggestions to develop online safety initiatives within school are considered. The adult members of the group are responsible for keeping up-to-date with latest risks, engaging with parents about matters surrounding online safety and monitoring the online safety incident log. The minutes of the Online Safety Group meeting are sent to the headteacher.

### **Roles and Responsibilities - Teachers**

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach Computing, ICT and Digital Citizenship and to use ICT resources within their class. This will be in accordance to the overviews provided by Rising Stars scheme of work. They will also assist in the monitoring and recording of pupil progress in Computing, ICT and Digital Citizenship. Teachers should also respond to, and report, any online safety or cyberbullying issues that they encounter within or out of school in accordance to online safety procedures as listed below. Teachers have a responsibility to report any problems with Computing resources to the ICT technician with a clear outline of the problem. Wherever possible, teachers should check that the Computing resources work and have the required software a week before their lesson, so the ICT technician can solve any problems that arise.

Whilst checking of personal sites, e.g. email, is permitted during non-contact times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and

ensure they are logged off appropriately (of both the website and their computer). Staff should follow, and agree to, the Acceptable Usage Policy below.

### **Roles and Responsibilities - The School**

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the Internet and ICT resources can be used safely, responsibly and respectfully. We will always ensure that we provide children with the opportunities to excel and achieve when using ICT resources and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events. A range of online safety websites, and our online safety overviews, will be made available on the school website.

We will conduct an annual survey of parents and pupils to ascertain Internet use at home. We will publish results from this in the school newsletter and on our website.

### **Roles and Responsibilities - Pupils**

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use Computing resources appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy as stated in the school's behaviour policy. Children should use their Google account for learning use only. If the children fail to do so, then the procedures outlined in these policies will come into force.

### **Roles and Responsibilities - Parents**

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about online safety and the use of the Internet. If they have any questions or concerns then they should speak to their child's teacher, the Computing coordinator or the headteacher.

### **Equipment, Hardware and Software**

Hardware should not be installed without the permission of the headteacher and/or ICT technician. The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the headteacher and/or the ICT technician for advice. The school reserves the right to examine or delete any files that are held on its system including on the shared Google Drive.

Full-time teaching staff are given a laptop to use, but other staff who need to, including supply teachers, may borrow one from the trolley providing this is signed in and out. Laptops from the

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

trolley should not be taken home without explicit permission from the headteacher and/or the ICT technician. To use the internet at home, teachers will need to change the Internet settings as required. Please note, school Computing resources which are taken home are only to be used by the person who has signed for it, other family members are not permitted.

### **Network**

Staff will be issued with a user account for the computer consisting of first name, last name and a simple password. It is their responsibility to change this in accordance with the password procedure below.

Pupils in the EYFS will not be expected to login to the computers and this may be done for them. Children from Year 1 upwards will be given an individual login consisting of their first name and first initial if necessary. Children in Key Stage 1 use a shared password and they will be able to set their own password when they are able to memorise it independently or at the latest as they move into Key Stage 2. These accounts will be created and monitored by the Computing coordinator or ICT technician.

There are two levels of user on the school laptops system, user , teacher and admin. Children should be using the normal user access which has software and resources suitable to their age-range differentiated by the different trolleys of laptops in each phase. The admin account should be reserved solely for the Computing coordinator and ICT technician to use for administrative tasks.

The school has a wireless network. The password for this is available for staff on request. Staff may connect their own devices to this network providing that the owner of the device consents to the headteacher and/or ICT technician checking the device if necessary. If the password is provided on paper, it should be destroyed once it has been used.

### **Backups**

The school's 4 (2 x office, 1 x business manager, 1 x headteacher) Windows-based administrator computers, which contain information such as the SIMs database, are backed up each night and stored securely off-site by MK Council The school's library system, which contains children's full names and classes, is backed up by Micro Librarian Systems (MLS) and stored offsite. Teacher's planning is backed up via the Google Drive's security measures and stored across encrypted Google servers.

### **School Website and Blogs - Linked to 360Safe Public Facing and Professional Standards Guidelines**

The school website will be overseen by the school administrator and it is expected that certain pages will be updated by other members of staff and children. The current website uses School Jotter and is hosted by Web Anywhere. The Computing blog is hosted on edublogs.com.



## Google Apps

The school's online learning space will be a system based around Google Apps for Education and Purple Mash. This is a free system that contains a number of tools including email, document sharing and website creation. All KS2 will be given an individual login and children in KS1 will use a shared year group login that will be given permission to use different tools according to their age and digital citizenship awareness. Children may need to prove that they can use tools safely before having them enabled. This will all be managed by the ICT technician with consultation with the Computing coordinator. Google have completed the self-certification checklist as provided by the DoE October 2014 in Cloud (Educational Apps) Software Services and the Data Protection Act to demonstrate their role with regards to the safety of information stored on their servers and have rated the majority of standards as being met entirely, with a small number not able to confirm.

## Internet and E-mail

The Internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the Internet unattended.

The teaching of email and Internet use will be covered within the ICT and Digital Citizenship curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the Internet.

All members of teaching staff will be issued with a school email address and this is the email with which they should use for professional communication. Other members of staff may have an email address if deemed necessary by the headteacher and/or the ICT technician. Children will also be issued with an email address on entering Key Stage 2 and this should be monitored by the class teacher, ICT technician and the Computing coordinator. Staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the ICT technician so it is the user's responsibility to ensure they log off appropriately. If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the ICT technician who will investigate.

The use of the Internet to access content such as auction sites, pornography, racist or any other inappropriate material is prohibited. If users, especially children, do see an inappropriate website or image, they should minimize this immediately and report the site to the ICT technician using the web-form provided on the school website or by discussing this with their class teacher.

When a staff member leaves the employment of the school, the staff member's email account and access to the Google Drive will be suspended on their last working day.

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

The Internet is provided by Turn IT On and the filtering is provided by the Exa Networks and the ICT technician will run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by Surfprotect run by Exa Networks. Additional sites can be enabled, disabled and blocked by the ICT technician and a record will also be kept of the sites enabled by school.

### **Passwords – Linked to 360Safe Password Guidelines**

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

For online services used in school such as blogs, Twitter , Viddler, Wallwisher and Animoto, an account per class is advised with a shared password across the school. It is important that these details are not given to pupils at any point, with the exception of Digital Leaders who may have access to additional services to assist them with their role.

For sites where children have their own passwords, e.g. Purple Mash, they will be provided with these by the ICT technician or Computing Coordinator. As children progress through the school, they will be taught about having sensible passwords for tools such as Google Apps.

### **School Liaison, Transfer and Transition**

When a new child joins, it is the responsibility of office staff to inform the ICT technician of the child's name and year group. The ICT technician will then provide accounts for the online tools available including the library system.

At the end of a child's time with us, they will be able to take their schoolwork with them should they wish by downloading their files from Google Drive at home. Photographs will be checked to ensure we have permission to share them before this takes place.

Once they have left our school, the child's account will be removed from the online tools and their content will be removed. This will happen the September after they leave. If any children do use the tools throughout the summer holiday, they must understand that this can be removed at any time.

### **Mobile Phones and Handheld Devices – Linked to 360Safe Mobile Phone Guidelines**

Staff may attempt to connect their phone to the school's wireless network in accordance with consultation with the ICT technician but should be aware that this may not work due to the settings available on their phones. It is not the responsibility of the ICT technician to ensure personal devices work on the school network.

## Age Limits

Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.

As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will also post details of these sites on our school webpage. We will ensure that these will tend to be sites that allow creation of content rather than searching other users' content.

Occasionally, these sites will be used by teachers with a class, for example to create a class book or movie. We currently use the following websites that children may have an individual, class or school account.

- Scratch 3.0
- TT Rockstars
- Story Jumper
- Soundtrap
- Education City
- Storyboard That
- Canva
- Animaker
- Tinkercad

We will make parents aware of this during our online safety events. If they do not wish their child to access these sites, their child can be provided with an alternative, non-ICT, method to complete the task.

## DATA

### Target Tracker

Our school uses Target Tracker. Within Target Tracker, our school account contains information that allows us to track the progress of our children and it enables us to provide appropriate comparative and benchmarking data to create meaningful reports relating to progress and attainment. Details of specific classes, groups or students are never released without permission of the Headteacher or Deputy Head.

Target Tracker aggregates data for statistical analysis and research, which may be published and used to provide comparative data to other schools and bodies interested in education.

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

The following data is stored for each student: UPN (Unique Pupil Number), Surname, Forename, Date of birth, Year Group, Date of Entry, Gender, FSM (Free School Meals), Pupil Premium, Ethnicity, First Language, EAL (English as an Additional Language), SEN (N- No special educational need A- School or Early Years Action P- School Action Plus S- Statement of SEN E- Education and Health Plan K- SEN Support), Gifted, Talented, In Care, Class, Preschool Exp (Number of terms before Reception), Previous Setting, Age, Terms Completed (Number of terms in setting), Attendance data, Transfer School data, school entered pupil notes, Postcode.

Assessment data is stored relating to teacher assessments, tests and progress through Assessing Pupil Progress. Children's data supplied by Caroline Haslett, does not contain email or postal addresses other than the postcode. Student Data is exported from SIMS. Data is then added by Caroline Haslett or by Target tracker on our behalf. We control our own Student Data, and can add, modify and delete student data. Target tracker only stores our Pupil Data when there is a formal agreement between us. Data from our school would be deleted within a year should we choose to end our subscription.

Pupil data is stored on a secure server using encryption and firewalls to protect the information from being accessed by anyone else. Periodically, an external company carry out a penetration test. Caroline Haslett has an encrypted security key so that only those with the key can access our school data. In addition, some school staff are assigned passwords that protect access to the system. Only members of our SLT staff can access this Data. No third party can access it without permission.

### **Personal Data**

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information onto personal devices.

### Social Media - Linked to 360Safe Social Media Guidelines

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils or their parents as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community (such as children's parents) and just ask that these members of staff take extra precaution when posting online
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- Inform the senior management team of any publically online links where you directly mention the school, or publications that list the school as your place of employment
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening
- Not use these media to discuss confidential information or to discuss specific children
- Check with the Computing coordinator if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school, we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.

We will use blogging throughout the school to share children's learning and to communicate with parents. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post on the blog or write a comment without it being approved by a teacher to ensure that the children are not subjected to any inappropriate comments. Spam messages (often containing inappropriate links and language) are caught by software installed on the blog (akismet) and this is monitored by the Computing coordinator. This is also updated regularly.

As part of our annual survey to parents and pupils, we will ask them on their use of social media to ascertain the number using sites such as Facebook as well as the popularity and usage of our Twitter feed.

### Digital and Video Images - Linked to 360Safe Digital and Video Guidelines

As a school, we will ensure that if we publish any photographs or videos of children online, we:

- Will try to ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the Computing Coordinator. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online

Staff should not use personal cameras or phones to take photographs of children within school.

### Technical Support

Many minor issues are dealt with by the ICT technician, Computing coordinator and the Digital Leaders as appropriate.

Additional hardware support is provided as and when necessary by Lynx Data Cabling.

Support for the website is provided by Web Anywhere.

Additional office-based support (e.g. MIS, SIMs) is provided by the Silverbug who offer remote desktop and telephone support when needed.

The school's library service is hosted by Micro Librarian Systems (MLS) who are responsible for its upkeep.

### Sustainability and Environmental Impact – Linked to ICT Mark 1b4

To ensure that the level of ICT resources across the school is sustainable, the ICT technician is responsible for the upkeep of all usernames, passwords and guides to online tools and software as well as details of licenses and a complete ICT resource inventory.

Hardware is disposed of safely and securely through [weee-stop.co.uk](http://weee-stop.co.uk).

### Online safety and its role in Digital Citizenship – Linked to 360Safe Online safety Guidelines

At Caroline Haslett we take Online safety and Digital Citizenship very seriously. We will ensure that it is taught often throughout the children's lessons as necessary. We will also provide children with dedicated Digital Citizenship lessons where appropriate. All Digital Citizenship overviews and

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

resource links will be available on the school website for parents to view. These will be reviewed regularly to ensure that they are up-to-date and reflect current needs. Children will be taught how to act online and how to minimise the risk when working on the Internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual Digital Citizenship focussed parent meeting and will provide regular updates via our website and newsletters as appropriate.

All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the ICT technician. All staff will also complete an AUP. Our own school's ICT Code of Conduct will also be posted in each classroom and on the trolleys to ensure they are seen by children and visitors.

Online safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online. The online safety training program will be split into three parts: 'Digital Citizenship curriculum', 'Digital Technologies Policy: what staff need to know' and 'Online safety: what to look out for'. Staff training will be reviewed annually and staff can always review resources from previous training sessions in the Subject Coordinators folder on Google Drive.

If there is a website available to children that staff or children deem inappropriate, they can either email the ICT technician or speak to the Computing coordinator who will then add it to the blocked website list on the school filters to block access in school.

If a teacher suspects an Online safety issue within school, they should make notes related to the incident in accordance to behaviour policies. This should then be reported to the senior management team and/or Computing Coordinator and recorded as appropriate.

If children receive an email that they believe to be inappropriate, then they should forward it on to their teacher and/or the ICT technician who will investigate.

On all school blogs, the website and within Google Apps, children will be provided with a button/page to report a problem to the ICT technician, Computing coordinator and deputy head should they find something inappropriate.

### **Complaints**

Incidents regarding the misuse of the Internet by students will be delegated to the Computing Coordinator who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

### **Copyright and Intellectual Property Right (IPR)**

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the Internet. In year 3/4 they will have discussions about the proper use of images with questions such as 'Is it OK to use an image we find online?' As they progress to year 5/6 some children should start referencing the sites they have used. This could be as simple as putting the name of the site the image came from or a hyperlink. It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the internet without some thought on their use.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This is in accordance with guidelines laid out by the local authority.



### Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

### Responding to unacceptable use by pupils

Pupils should be aware that all online safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy that includes the anti-bullying policy. Children may have restrictions placed on their account for a short time.

## Our Remote Learning Policy.

### Teachers

When providing remote learning, teachers are responsible for:

#### *Setting work:*

- For Foundation and Year 1 classes, teachers will provide a range of resources through Tapestry that children will be engaging with.
- For Key Stage 1 and 2 classes, teachers will provide activities through Google Classroom Daily Live Lessons of around an hour are to be set for English and Mathematics, other activities should enable children to engage each foundation subject at some stage each week.

#### *Submitting work and providing feedback on:*

- Children in Key Stages 1 and 2, when completing work within Google Classroom will receive written feedback regarding their progress through private comments.

### Teaching assistants

When assisting with remote learning, teaching assistants are responsible for:

- attend live lessons when possible.
- Will liaise with class teachers to support planning and resourcing differentiated learning.

- Provide private comments on children's tasks when necessary.

### Pupils and parents

Staff can expect pupils to:

- Be contactable during the hours of the school day 9am – 3pm
- Seek help from teachers if they need it.
- Alert teachers if they're not able to complete work

Staff can expect parents to:

- access Google Classroom/Tapestry
- Seek help from the school if they need it.
- Be respectful when making any complaints or concerns known to staff

If parents have any questions regarding work that has been set they should contact their child's class teacher in the first instance.

### Governing board

The governing board is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible

### 3. Who to contact

If staff have any questions or concerns about remote learning, they should contact the following individuals:

Here are some suggested issues and the most likely points of contact, but adapt and add to this as needed:

- Issues in setting work – talk to the relevant Team Leader / Assistant Head
- Issues with behaviour – talk to the relevant Team Leader / Assistant Head
- Issues with Computing Equipment or Google Classroom – talk to/ log an issue with Computing Coordinator /ICT technician

- Issues with their own workload or wellbeing – talk to the relevant team leader / Assistant Head
- Concerns about data protection – talk to the Data Protection Officer
- Concerns about safeguarding – talk to the Deputy Headteacher who is Designated Safeguarding Lead

#### 4. Data protection

##### **Keeping devices secure**

All staff members will take appropriate steps to ensure their devices/accounts remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

#### 5. Safeguarding

The safeguarding and child protection policy for the school has recently been updated to reflect current expectations linked to promoting safeguarding in the context of Covid-19. This can be accessed on both the school website and the Grand Union Partnership website.

#### 6. Monitoring arrangements

This policy will be reviewed on a monthly basis and updated when required by the Headteacher/Computing Coordinator. When updates need to be made to make sure that the policy is in step with government guidance they will be approved by the governing body.

## **Our Acceptable Usage policy for Live Lessons during the Coronavirus Pandemic**

### **TEACHERS**

- Teachers may host live lessons where and when they find this will enhance the learning experience for the children.
- Teachers will send the invite to children for the live lesson the morning of the scheduled lesson.
- Teachers will be dressed appropriately and remain professional throughout the video.
- Teachers will ensure no other family members are in view of the camera.

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

- All videos will be **RECORDED** for safeguarding purposes. These are stored automatically on the school's Google Drive account.
- No video lessons will be one-to-one. If only one student turns up for the meeting, a reminder message will be sent. If no one else arrives after the reminder, the teacher will need to end the meeting.

### **CHILDREN**

- Children must be dressed appropriately for the duration of the video lesson.
- Children must remain on mute until invited to speak.
- Children are prohibited from recording or capturing/screen grabbing content from the video call.
- Children should remain in a public part of their house wherever possible.
- Devices should not be used in the bathroom/bedroom or anywhere in the house your parents do not give permission.
- Children may be muted during the lesson
- Children may have their school Google Accounts suspended if they behave inappropriately.

### **PARENTS**

- Parents should ensure their child is appropriately dressed for sessions.
- Parents should ensure that their child is aware of the need to behave in a session delivered by video link in the same way as if they were in school with the member of staff. If a student is behaving inappropriately, we may suspend their school google account.
- Parents should ensure other family members are out of camera shot and do not contribute to the video call.
- Parents should ensure their child is familiar with how the whole process works.

### **Guidance and support for Parents and Carers**

Please let your children have some privacy. Children will need to be able to participate without worrying about you overhearing them, so let them set up in a location that offers this opportunity if possible.

Plug your device in if possible and close unnecessary tabs. It is a good idea to keep devices plugged into the mains power.

Set expectations for how your child should behave on camera: Face the screen; mute yourself when you're not speaking; unmute yourself when you're ready to talk; turn off the camera if you need to blow your nose; etc.

Children should behave appropriately when learning by video, just the same as if they were in the classroom.

Please have equipment available. Children may need earphones, a microphone, and paper

or pencils to take notes. Children may need extra resources from Google Classroom in advance.

Choose a neutral background where possible. Children should not be in their bedrooms or in the bathroom.

Just as with everyday school, children should go to the toilet before the session. If there's an emergency, make sure your child knows how to temporarily disable the video and mute themselves and then turn everything back on again.

Be respectful of others.

Remind the children that this is an unusual time for everyone, and appropriate behaviour should be maintained at all times.

### **Our Safe use of Photos**

Caroline Haslett Primary School, in common with all other schools, needs and welcomes positive publicity. Children's photographs add colour, life and interest to materials and articles promoting school activities and initiatives. This can increase pupil motivation, staff morale and help parents and the local community identify and celebrate the school's achievements.

However, in order to respect young people's and parents' rights of privacy and because of potential child protection issues, photographs must be used in a responsible way. Caroline Haslett Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share in this commitment.

This policy seeks to achieve a practical balance to secure the above.

#### **Data Protection Act**

Under the terms of the Data Protection Act 2018 images of pupils (or staff) must not be displayed in a public place without consent. This includes publications such as the school prospectus, website or areas in the school where visitors have access.

#### **General rules on using photographs of individual children**

On entry to school in Foundation stage or when pupils are admitted mid year, parents will be asked to complete a consent form.

A check **MUST** be made to ensure that children are not on the school list of those whose photographs must not be used before publishing in documents or on the website.

Images of children in suitable dress will be used – photos of children engaged in swimming present a greater risk of potential misuse and will not be used.

## DIGITAL TECHNOLOGIES POLICY

Date of Issue: December 2020

Where we have been informed that a child is subject to a court order then we will never use their image.

We will ensure images are stored securely, especially where electronic, and used only by those authorised to do so.

Ensure file names given to electronic images of pupils do not identify the child - e.g. maryjones.jpeg

### Newspapers

As long as parental consent has been secured newspapers may publish photographs of pupils, but must not publish names alongside them. They may however refer to group photographs collectively e.g. Class AB or Caroline Haslett Primary School Year 6 football team.

Pupils must not be approached or photographed whilst at school (or engaged in school activities outside school) without the permission of a member of staff.

### Video & Filming

The appropriateness of photographic images earlier outlined also applies to video/film images.

We recognise that parents, carers and family members wish to record events such as school plays, sports days etc to celebrate their child's achievements. However it is important that such records remain private and for their own personal use if they include children other than their own. Under no circumstances should parents/carers post video footage or still images of children other than their own on any publicly accessible internet site. To do so may place the individual responsible in breach of the Data Protection Act. This restriction applies to any footage/images taken on the school site or during school-led off-site activities. Upon a child's admission to the **school parents will be asked to sign a photography consent form that acknowledges this.**

### Tapestry

In Foundation and Year 1, an online system called Tapestry is used to record and store all observations and assessments relating to each child. Parents are asked to sign a consent form permission for their child's image to appear in other children's Learning Journeys, and to protect images of other children that may appear in any photos contained. If parents withhold this consent their child is only ever photographed alone and no shared observations are made including that child. Parents can share these photographs with their child, family and friends at home and also post any comments and photographs of their own. Staff use tablets to take the photographs for observations which are be uploaded to the journals. Each teacher has a secure

## **DIGITAL TECHNOLOGIES POLICY**

Date of Issue: December 2020

login which is password and pin protected.

### **Commercial & Outside Photographers**

Will be given a clear brief about what is considered appropriate in terms of content and behaviour.

Wear identification at all times.

Will not have unsupervised access to children or one-to-one photo sessions.

### **Parental Consent**

Parents are requested to inform school if they do NOT wish their children's pictures to be used in publications or on the website and an up to date register of those children is maintained.

### **Complaints Procedures**

Parents should follow the school's normal parental complaint procedures in most cases. In the case of concerns regarding the use of photographs by the press, they should contact the Press Complaints Commission or the Office of Communications (OFCOM) in the case of TV companies.

### **Review**

This policy will be reviewed by the Governing Board in line with the Child Protection Policy, in view of the continual advances in technology and in response to significant views expressed by parents, staff and pupils (if appropriate).

## Appendix A

### CAROLINE HASLETT PRIMARY SCHOOL PRIMARY SCHOOL

#### Consent Form: Use of Photographs

Name of Child:

Date of Birth:

**Caroline Haslett Primary School** would like to take photographs and or video recordings of pupils whilst they attend the school to celebrate their achievements and successes. Still images may be published in our printed publications [e.g. school prospectus, newsletters] and both still and moving images may be used on our website [[www.haslett.org.uk](http://www.haslett.org.uk)]. They may also be used to promote the good educational practice of the school to other teachers, e.g. at training events organised by the Local Education Authority or national education/government institutions. Children's names will never be published alongside their photograph externally to the school. Names may be used internally, for example – on a display.

Photographs / videos may also be published for internal use only, as part of children's regular classroom work e.g. on classroom displays, within multimedia projects (e.g. PowerPoint), on the school's internal network and to share educational achievements with parents, e.g. video presentation of a school trip. Electronic images, whether photographs or videos, will be stored securely on the school's network which is accessible only by authorised users.

Before using any photographs/videos of your child we need your permission. Please answer questions 1 to 5 below, then sign and date the form where indicated.

**Please return the completed form to the school office as soon as possible.**

Please delete as appropriate

1. May we use your child's photograph in printed publications produced by Caroline Haslett Primary School Primary School [e.g. school newsletters] or Milton Keynes Council? **Yes / No**
  
2. May we use your child's photograph on our website/Google Classroom:
  - a) as part of a large group or whole school activity? **Yes/No**
  - b) showing an individual activity? [e.g. holding a winner's trophy] **Yes/No**



## DIGITAL TECHNOLOGIES POLICY

Date of Issue: December 2020

3. May we allow your child's photograph [e.g. as part of a school team or record of a school event] to be used for publication in a newspaper? **Yes / No**

4. May we use any photograph or video of your child internally as part of the regular curriculum and work of the school? **Yes / No**

5. May we use any still image or video containing your child to share good educational practice with teachers from other schools? **Yes / No**

This form is valid from the date of signing until your child leaves the school.

Photographs and videos may be securely archived after your child has left the school. Archiving provides a valuable record of the school's history for future generations. We recognise that parents, carers and family members will wish to record events such as school plays, sports days etc to celebrate their child's' achievements.

Caroline Haslett Primary School is happy to allow this on the understanding that such images/recordings – if they include anyone other than your child – are used for purely personal family use.

**In signing below, you are agreeing to abide by this restriction.** Any parents/carers who are found to be in breach of this restriction will be not be permitted to take further photos/video footage on the school site.

A full copy of the school's policy on the safe use of children's photographs may be viewed on the school website or obtained upon request from the school office.

Signed:

[parent/carers] Date:

### CHPS Acceptable Usage Policy – Staff – Linked to 360Safe AUP Guidelines

This document has been written to ensure that staff use the Computing resources throughout the school appropriately. If they have any questions regarding this policy, they should direct them to the senior management team or the Computing coordinator. Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines, carry the machines carefully with two hands
- Ensure that they have a sensible password
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer – particularly when their computer is left unattended e.g. during breaks and lunchtimes
- Make use of resources such as cameras but ensure that these are returned after their use. They should also endeavour to remove pictures/files regularly
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that personal online devices are used in a childfree area and whilst off duty. Personal devices should be locked away during the school day.
- Be aware that if a personal device is used in school, that device can be subject to the inspection of the headteacher and/or ICT technician.
- Ensure that any online activity on school devices should be related to their professional duty and that personal use should be kept to a minimum
- Be aware that use of material related to violence or extremism is strictly prohibited.
- Ensure that they are not using the school's ICT resources for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the Digital Technologies Policy
- Be aware that software or hardware should not be installed without prior consent of the ICT technician or headteacher
- Be aware that personal cameras or phones should not be used to take photographs of our children.
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the headteacher
- Where data of a personal nature such as school reports, FACTs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the General Data Protection Act (May 2018) and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
- Report any issues with ICT resources to the ICT technician as soon as possible and ensure the problem is clearly outlined

## DIGITAL TECHNOLOGIES POLICY

Date of Issue: December 2020

- Take responsibility for the online safety of the children and ensure any issues, incidents, or potential incidents, are reported straight away to the senior management team and/or the ICT technician and make notes related to the incident in accordance to behaviour policies.
- Return any hardware or equipment if they are no longer employed by the school

Signed \_\_\_\_\_ Print \_\_\_\_\_ Date \_\_\_\_\_

\_\_\_\_\_

### Acceptable Usage Policy KS2 Children – Linked to 360Safe AUP Guidelines

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computing resources. By using the Computing resources in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher Mrs Hart or Mr **Bazeley**.

- At all times, I will think before I click
- I will only use the Computing equipment for what I've been asked to use it for
- When using the Internet, I will think about the websites I am accessing
- If I find websites, information or images which are inappropriate or make me feel uncomfortable, I will tell a teacher or a trusted adult straight away and no one else.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (instant messaging, email etc), I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will not share personal details such as my surname, school name, home address, email address or phone number
- **I will not use my school email address to sign up to online accounts without asking my teachers.**
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not login to another person's account
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around the school building
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

Signed (Pupil) \_\_\_\_\_ Class \_\_\_\_\_ Date \_\_\_\_\_

**Acceptable Usage Policy KS1 Children – Linked to 360Safe AUP Guidelines**

These rules have been written to make sure that you stay safe when using the computing resources. By using the Computing resources in school, you have agreed to follow these rules. Mrs Hart will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher, Mrs Hart or Mr **Bazeley**.

The Golden Rule: **Think before you click**

- 😊 I will be careful when going on the Internet.
- 😊 I will only use the Internet when a teacher is with me.
- 😊 I will tell a teacher if I see something that upsets me.
- 😊 I know people online might not be who they say they are.
- 😊 I will be polite when talking to people or writing online.
- 😊 I will think before I print or delete.
- 😊 I will be careful when using or carrying equipment.
- 😊 I will keep my password secret, but I can tell my family.
- 😊 I will remember to log out properly before closing the lid of the computers.
- ☹ I won't tell anyone any personal details like my phone number or last name.
- ☹ I won't login using someone else's username.
- ☹ I won't put water bottles on the table when using ICT resources.

Signed (Pupil) \_\_\_\_\_ Class \_\_\_\_\_ Date \_\_\_\_\_

\_\_\_\_\_

**Acceptable Usage Policy Foundation Stage – Linked to 360Safe AUP Guidelines**

By using the ICT resources in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents. If you have any questions, please ask your teacher, Mrs Hart or Mr **Bazeley**.



These rules help you to stay safe when using the computers.

- 😊 I can use the computer in independent play.
- 😊 I will only use the programs or apps a teacher has said I can use.
- 😊 I will tell a teacher if I see something that upsets me or I do not understand.
- 😊 I will think before I click.
- 😊 I will be careful when using or carrying equipment.



Signed (Pupil) \_\_\_\_\_

Class \_\_\_\_\_ Date \_\_\_\_\_

## **Acceptable Usage Policy Governors and Visitors – Linked to 360Safe AUP Guidelines**

Visitors, both physical and virtual, may be provided with accounts to our network and/or online systems. Visitors will have a lower level of access than staff and each account will be provided on a case-by-case basis. This will depend on the purpose of the account requested. Supply teachers will be listed as visitors to the school, unless it becomes a long-term placement.

### **Online Systems** (Purple Mash, Google Apps, school website)

Visitors must provide the ICT technician with their name and email.

Users will:

- Have access to the Google Apps homepage, documents and sites
- Not have access to mail or direct contact with children (unless strictly necessary)
- Understand that this account may be removed at any time so should not use it to save vital information

### **School Network and wireless**

Users will:

- Be given a login for their time in the school
- Be expected to follow the guidelines as set out for staff
- Understand that this account may be removed at any time
- Be provided with the wireless key and guidelines for connecting to the network