Caroline Haslett Primary School

& Faraday Club

DIGITAL TECHNOLOGIES POLICY

Date of Issue: September 2024

Date of next review: September 2025 (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: _____

Introduction

The use of computers and computer systems is an integral part of the National Curriculum and knowing how they work is a key life skill. In an increasingly digital world there now exists a wealth of software, tools and technologies that can be used to communicate, collaborate, express ideas and create digital content. At Caroline Haslett Primary School, we recognise that pupils are entitled to a broad and balanced computing education with a structured, progressive, approach to learning how computer systems work, the use of Digital Devices and the skills necessary to become digitally literate and participate fully in the modern world. The purpose of this policy is to state how the school intends to make this provision.

This policy aims to cover the different elements that Computing, Information Communication Technology (ICT) and Online Safety 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. Online Safety 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 Online Safety 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. Often schools will have a number of policies including Online safety, Mobile Phones, Computing and Social Media, but as a school we have decided to combine them into one policy.

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 Online Safety 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
- 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

ONLINE SAFETY

Contents

1. Online Safety Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, online safety-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Jo Cleary.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Computing Lead to make sure the appropriate systems and processes are in place
- Working with the headteacher, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of online bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Computing Technician

The Computing technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of online bullying are dealt with appropriately in line with the school behaviour policy

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's Computing systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
- Following the correct procedures by contacting the Turn It On ticket system if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of online-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Understand that their child will read and agree to the terms on acceptable use of the school's Computing systems and internet annually

3.7 Visitors and members of the community

Visitors and members of the community who use the school's Computing systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use..

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

- Relationships education and health education in primary schools

In Key Stage (KS) 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage (KS) 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of online safety in newsletters or other communications home, Online Safety Evenings, Wellbeing fairs and in information via our website or virtual learning environment (Google Classroom). This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Online-bullying

6.1 Definition

Online-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing online bullying

To help prevent online-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss online-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss online-bullying with their classes and it will be discussed regularly in online safety lessons.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on online-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on online-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Caroline Haslett recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Caroline Haslett will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 4). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 4.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day or on the school premises.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 2 and 3).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices 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 their 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
- Ensuring the Computing technician installs anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Computing technician.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behavior policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures or staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including online bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, onlime bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Internet acceptable use policy

G Suite for Education (inc. Classroom)

Privacy Information

At Caroline Haslett Primary School, G Suite for Education is used and a G Suite for Education account for every child is managed. G Suite for Education is a set of education productivity tools from Google that include Gmail, Calendar, Docs and Classroom, amongst many others. These are used by tens of millions of pupils and teachers around the world. An Education account means that data is not collected for advertising purposes and no adverts will appear whilst a pupil is using these tools.

At Caroline Haslett Primary School, children will use their G Suite accounts to complete assignments, communicate with their teachers and learn 21st century Online Safety skills.

The notice below provides answers to common questions about what Google can and cannot do with your child's personal information, including:

● What personal information does Google collect?

● How does Google use this information?

● Will Google disclose my child's personal information?

● Does Google use pupil personal information for users in primary and secondary schools to target advertising?

● Can my child share information with others using the G Suite for Education account? Please read it carefully and if you have any questions please contact the school and let us know.

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from pupils in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google described at: https://gsuite.google.com/terms/user_features.html

- Classroom – Used for presentation of resources, classroom and homework assignment, marking of work and feedback
- Docs - word processing
- Forms - survey and quiz tool for subjects and school
- Slides – presentations
- Calendar – personal school calendar
- Contacts – for communicating with teachers and their classes etc
- Drive – Storage of pupil files
- Groups – for organisation of class groups
- Keep – note taking
- Sheets - spreadsheets
- Sites – creation of website under direction of teacher / subject only
- Meet - under direction of teacher / subject only
- Vault – storage/backup facility In addition, we also allow pupils to access certain other Google services with their G Suite for Education accounts. Specifically, your child may have access to the following "Additional Services":
- YouTube - Education account only (No adverts)
- Maps
- Google Earth

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html

You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a pupil account, Caroline Haslett Primary School may provide Google with certain personal information about the child, including their name, school (G Suite) email address, and password. When a pupil uses Google services, Google also collects information based on the use of those services.

This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
- log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings. How does Google use this information?

In G Suite for Education Core Services, Google uses pupil personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in primary schools to target advertising? No. For G Suite for Education users in primary schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using a G Suite for Education account.

Can my child share information with others using the G Suite for Education account? We may allow pupils to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organisations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- With Caroline Haslett Primary School. G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons. Google will share personal information with companies, organisations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: - meet any applicable law, regulation, legal process or

enforceable governmental request. - enforce applicable Terms of Service, including investigation of potential violations. - detect, prevent, or otherwise address fraud, security or technical issues. - protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

- Google also shares non-personal information – such as trends about the use of its services – publically and with its partners. What if I have more questions or would like to read further? In the first instance, you and your child can visit https://myaccount.google.com while signed in to the G Suite for Education account to view and manage the personal information and settings of the account. If you have questions about our use of Google's G Suite for Education accounts, please contact schooloffice@carolinehaslett.milton-keynes.sch.uk

If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review: The G Suite for Education Privacy Center https://www.google.com/edu/trust/ The G Suite for Education Privacy Notice https://gsuite.google.com/terms/education_privacy.html The Google Privacy Policy at https://www.google.com/intl/en/policies/privacy/ The Core G Suite for Education services are provided to us under Google's Apps for Education agreement https://www.google.com/apps/intl/en/terms/education_terms.html The Data Processing Amendment https://www.google.com/intl/en/work/apps/terms/dpa_terms.html

School Liaison, Transfer and Transition

When a new child joins, it is the responsibility of office staff to inform the Computing technician or the Computing Lead of the child's name and year group. The Computing technician or Computing Lead will then provide an account 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.

Once Year 6 have left our school, the children's accounts will be deleted 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. Should children transfer to another primary school their account will be suspended.

Appendices 1

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, SEN documents, 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
- 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 _____

Appendices 2

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. Your parents will be able to see these rules in Google Classroom. Failure to follow these rules may result in your account being suspended.

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

- 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 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 _____

Appendices 3

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. Your parents will be able to see these rules in Google Classroom. Failure to follow these rules may result in your account being suspended.

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

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 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 will not use a personal phone in school.

☹ 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.

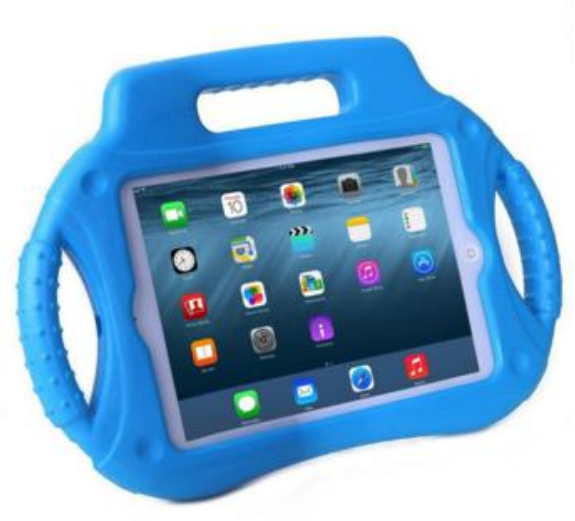
Signed (Pupil) _____ Class _____ Date _____

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 or Mrs Hart.

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 _____