	Computer Studies and Acceptable Use Policy Updated 05-19 Next Review 05-20 Prepared by: JUH/SHCC Authorised by: PAW/ISB

This Policy applies throughout the School from the EYFS to Year 6.

Introduction

This document is a statement of the aims, principals and strategies for the use of information and communication technology at the School.

Computer studies utilises a variety of systems that handle electronically retrievable information. Computers are the most obvious of these but computer studies also includes use of digital cameras, bee-bots, calculators and iPads.

Aims

Our aims in using computer studies and computer technology are that all pupils will have the opportunity to:

- Enjoy computer studies and tackle all applications with confidence and a sense of achievement
- Develop practical skills in computer studies and the ability to apply these skills to the solving of relevant and worthwhile problems
- Understand the capabilities and limitations of computer studies and the implications and consequences of its use
- Keep safe with a thorough knowledge of online safety, appropriate to their age

Principles

Computer studies is important because:

1) Its use is widespread in the modern technological world and likely to continue to grow and it is an important medium for learning and study at all educational/workplace levels. The relevance of computer studies to pupils' lives, personal experiences and futures gives them motivation to succeed in the subject and makes learning enjoyable for them. Computer studies contributes to developing successful learners by providing powerful tools for developing creativity, initiative and independent thinking. Computer studies helps pupils to follow enquiries and solve problems, and enhances their skills in logical reasoning, questioning, analysis and research.

2) Computer studies develops pupils' independent learning skills and their confidence, and provides a variety of ways for them to present and share their knowledge and ideas. The subject supports communication and collaborative working.

In September 2014 a new computing curriculum was launched. The National Curriculum for Computer Studies aims to ensure that all pupils:

- Can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- Are responsible, competent, confident and creative users of information and communication technology

(Department for Education, 2014)

Computing is also seen as a cross-curricular strand in the National Curriculum and indications for its use are given in most subjects.

In the EYFS, computer studies comes under the category of Technology within the Understanding the World area of learning.

As a school we are aware that this area of the curriculum requires updating frequently to ensure staff knowledge and competency with hardware and software reflect the evolving progress in this area. The skills that pupils are capable of have moved on from when the previous National Curriculum and QCA Schemes of Work were published. Bearing this in mind we are always looking at ways of using new software to implement a more cross-curricular Computing curriculum). Regular retraining is carried out by the Computer Studies Educator and staff from the Camden Learning Centre (CLC). Pupils from different year groups regularly visit or are visited by the CLC.

The Computer Studies Educator is Paula Webb Murphy, who will undertake CEOPS training at CLC and is able to advise staff on current guidelines and good practice related to online safety.

Strategies for the use of computer studies

Computer studies is taught both as a distinct subject and is also integrated when appropriate throughout the curriculum to support and enrich pupils' learning. In order to ensure that valuable areas of experience are covered:

- All classes will offer pupils experience in the use of computer studies
- Computer/laptop/iPad use is carefully managed so that all pupils are given equal access opportunities
- Computer studies use is offered as an entitlement for all pupils

Pupils with Special Educational Needs have the same, or in certain circumstances additional, computer studies entitlement as all other pupils and are offered the same curriculum. However, in addition, particular applications of computer studies are used for:

- Pupils with difficulties in learning, who need to be motivated to practise basic skills regularly and intensively, benefit from the use of programs in which skills practice is set in the context of a motivating game, such as Word Shark and Nessy Fingers. They can also use the dictation app on iPads
- Pupils of high ability who may be extended through the use of programs which offer challenge and opportunities for investigation, such as making an iMovie for Eco Week

The emphasis in our teaching of computer studies is on the use of computers/laptops/iPads as tools to support learning.

- All pupils are made familiar (at as early a stage as possible) with basic aspects of efficient use of keyboard and mouse pad
- Digital literacy is covered through the use of apps such as Book Creator
- Touch typing is introduced and developed from KS1 upwards
- Pupils are introduced to simple coding from Year1
- As pupils progress through the School they are given increasing control of their use of computer studies, gaining growing independence in their use of computer studies as a tool appropriate to any given activity and in their choice of software required.

Excellence in computer studies use will be celebrated in demonstrations and display including:

- Displays of text, pictures, graphs and charts which have been produced by pupils using computers/laptops/iPads

Strategies for ensuring progress and continuity

Planning for the use of computer studies is a process in which all teachers will be involved, where:

- Suggestions for computer studies activities are developed by the Computer Studies Educator in collaboration with colleagues
- Staff meetings may be used to discuss computer studies across the curriculum and ensure consistency of approach and of standards

The role of the Computer Studies Educator is to:

- Take the lead in policy development and the integration of computer studies into schemes of work designed to ensure progression and continuity in pupils' experience of computer studies throughout the School
- Support colleagues in their efforts to include computer studies in their development of detailed work plans, in their implementation of those schemes of work and in assessment and record keeping activities
- Monitor progress in computer studies and advise the Headteacher on action needed
- Take responsibility for the purchase and organisation of central resources for computer studies
- Take appropriate steps to keep up-to-date with developments in this rapidly changing field and pass on information to colleagues as appropriate
- Be aware of the current guidelines on the teaching and learning of online safety

Assessment

Feedback to pupils about their own progress in computer studies is rarely formalised and is usually given while a task is being carried out through discussion between pupil and teacher. Formative assessment is mostly carried out informally by teachers during their teaching. Suitable tasks for assessment of computer studies work include:

- Small group discussions perhaps in the context of a practical task
- Pupil self-evaluation in KS2 in conjunction with teacher supervision
- Electronic teacher assessment in KS1 and KS2 based on pupils' completed work
- EYFS assess progress made on an online system - Tapestry

- Specific computer studies assignments for individual pupils
- Individual discussions in which pupils are encouraged to appraise their own work and progress.

Strategies for the use of resources

Classroom resources for computer studies include:

- At least one computer in most classrooms
- A laptop trolley in St Luke's Building
- A laptop trolley in the Main Building
- A laptop trolley in St Mary's
- 3 iPads in the Gatehouse for the use of peripatetic music staff
- An iPad sync cart with 32 iPads for pupils and 10 iPads with Apple Classroom app for Staff in the Staff Room
- A set of calculators in each classroom upwards from Year 3
- Bee-bots to use for EYFS and KS1 pupils
- Brain trainers for various year groups to use

Staff are encouraged to prepare resources and develop personal competence and confidence in the use of computer studies.

iPads may be used as a teaching tool or as a staff management tool. Pupils should not be allowed unsupervised access to the internet on an iPad. iPads should be locked away or taken home by staff at the end of a school day.

Health and safety issues in computer studies include taking care with:

- Setting up and moving equipment
- Establishing appropriate working conditions
- General electrical safety

Acceptable Use Policy

This Policy applies to all members of the School community who use School IT systems, as a condition of access. Access to School systems is not intended to confer any status of employment on any contractors or service providers.

The computer system is owned by the School. 'The computer system' means all computers, memory sticks and other associated equipment belonging to the School, whether part of the School's integrated network, stand-alone or taken off-site.

Professional use of the computer system is characterised by activities that provide pupils with appropriate learning experiences and allow adults to enhance their own professional development. The School recognises that technologies such as the internet and email will have a profound effect on pupils' education and staff professional development in the coming years and the School's Online Safety Policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the School, whether legitimately licensed or not, is expressly forbidden.

The School provides staff with encrypted memory sticks.

The School reserves the right to examine or delete any files that may be held on its computer systems or to monitor any internet sites visited.

All pupils must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of internet use. They must sign an acceptable use statement agreeing to highlighted points (see Appendix).

If staff are using the internet on their own smartphones, iPads or Kindles, then the same internet access rules apply when staff are on School premises.

Internet Access Policy

The School cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

All internet activity should be appropriate to staff professional activities or the pupils' education.

The provision of School email accounts, WiFi and internet access is for official School business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their School IT use and limit as far as possible any personal use of these accounts. Please be aware of the School's right to monitor and access web history and email use.

All official School business must be conducted on School systems, and it is not permissible to use personal email accounts for School business.

Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person or publicly displayed

The internet may be accessed by staff and pupils during School hours.

Activity that threatens the integrity of the School's computer systems, or that attacks or corrupts other systems, is prohibited.

Users are responsible for all emails sent and for contacts made that may result in emails being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media. Staff should respond within 24 hours to emails sent during the working week where possible. Staff are not expected to respond to emails received after 16.00 unless they are of vital importance. Staff may, at their discretion, not respond to emails received during holidays/weekends until School resumes.

Use of the School's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.

Teaching staff should not use Google images searching while an interactive white board or computer is in view of pupils.

Any educational material viewed on YouTube must be viewed beforehand by teaching staff.

Social networking sites such as Facebook should not be accessed from School computer equipment. Staff may use their own personal smartphones or iPads to view such sites in the Staff Room.

Staff should be discreet when using their personal mobile devices in and around the School. Staff should not use their personal mobile devices when in class with pupils or in shared School areas (e.g. corridors, playground) during the course of the School day. Specific provisions for personal mobile devices apply to EYFS staff in accordance with the School's Safeguarding and Child Protection Policy.

Staff should not use their personal social networking sites to discuss confidential School matters or share pupils' work. Staff should not include parents or pupils as contacts on their social media sites.

Staff who use social network sites should have the highest level of privacy settings and ensure these are regularly updated.

Staff should not give pupils or parents and guardians their personal email addresses or reply to emails sent to their personal email addresses by pupils or parents and guardians.

Staff should not reply to individual emails that may have been sent to them by pupils; such emails should be forwarded to the Headteacher.

Staff should not email School material to their personal email addresses. If they need to work on School material at home, they should access it from their School email address via webmail or use encrypted memory stick provided by the School.

If the internet is used in whole School assemblies and in class then the material must be checked before viewing and any advertising/comments kept out of view of the audience.

Copyright of materials must be respected. When using downloaded materials, including free materials, the intellectual property rights of the originator must be respected and credited. All material saved on the School's network is the property of the School and making unauthorised copies of materials contained thereon maybe in breach of data protection law[1], individual copyright or intellectual property rights.

Use of materials stored on the School's network for personal financial gain is prohibited.

Posting anonymous messages and forwarding chain letters is prohibited.

The use of the internet, email, or any other media to access inappropriate materials such as pornography, racist, violent extremist or any other offensive material is forbidden.

The School is aware of its duty under Section 26 of the Counter-Terrorism and Security Act 2015 to prevent pupils from being drawn into terrorism (the 'Prevent Duty'). In accordance with the Department for Education advice *Protecting children from radicalisation: the prevent duty* (2015) the School ensures that suitable filtering is in place, that the risk of online radicalisation is incorporated into the curriculum and that all teaching staff are aware of the risks posed by the online activity of extremist and terrorist groups.

It is the responsibility of the user to ensure that they have logged off the system when they have completed their task.

[1] General Data Protection Regulation (EU 2016/679), the UK Data Protection Act 2018 and related legislation, The Privacy and Electronic Communications Regulations 2003 and the Protection of Freedoms Act 2012.

The teaching of internet safety is included in the School's computer studies and PSHCE scheme of work but all teaching staff within all year groups should be including internet safety issues as part of their discussions on the responsible use of the School's computer systems.

Each year the School will actively participate in Internet Safety Day.

Pupils in KS1 & KS2 understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff. Children in the EYFS will be supported to do so.

Experts in the field of computer safety come in to talk to pupils, staff and parents about how to keep safe online. We also consult these experts if we have questions or concerns about pupils' online safety. Updates on computer studies and online safety may be included the weekly newsletter.

Throughout the School, the majority of the access to the internet will be by teaching staff or other adult demonstration. However, there will be occasions, from Reception upwards, when pupils have supervised access to specific approved online programs such as Mathletics, Purple Mash, Conquer Maths and Nessy Fingers. Pupils may also access these programs from home. Parental consent for the limited use of pupils' personal data to set up the necessary accounts for these programmes is obtained and parents are advised to supervise their children's remote use of these programs.

Pupils in Years 1-6 will discuss safe use of the internet with the class teacher and will, with their parents' consent, sign an Acceptable Use Agreement. This will be signed each September and displayed in class. Children in the EYFS are supported to use the internet safely and to begin to gain an understanding of the importance of this.

Pupils using the internet in School will be appropriately supervised. All internet access is filtered through a proxy server to screen undesirable sites at source. Pupils will only use specific sites that have been vetted by teaching staff beforehand and will use child-friendly search engines.

Pupils using the internet in School should only use the internet in the presence of an appropriate member of staff. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet service provider via the Computer Studies Educator, the ICT Manager or the Bursar.

Pupils should not have access to chat rooms and should not engage in conversation or dialogue with other users on the internet at School.

Staff receiving suspicious emails containing attachments must not open them because of the risk of viruses. The Bursar or ICT Manager must be informed immediately if this happens accidentally.

Internet and system monitoring

All members of the School community should be aware that School email and internet usage (including through School WiFi) will be monitored for safeguarding, conduct and performance purposes, and both web history and School email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

All internet activity is monitored through the server. It is the responsibility of the ICT Manager to review this activity periodically. It is the duty of the ICT Manager to report any transgressions of the School's internet policy and/or use of obscene, racist, violent, extremist or threatening language detected by the system to the Headteacher. Occasionally, it may be necessary for the ICT Manager to investigate attempted access to blocked sites, and in order to do this, the ICT Manager will need to set his internet access rights to 'unrestricted'. Whenever this happens, it should be recorded in the ICT violations register and the Headteacher notified.

Breaches of this Internet Access Policy and use of inappropriate language by pupils can be dealt with in a range of ways appropriate to the severity of the offence, including: removal of internet access rights; computer system access rights; meetings with parents or even exclusion. This is in accordance with School's Behaviour Policy.

Breaches of this Internet Access Policy by employees will be reported to the Headteacher and will be dealt with according to the School's Capability and Disciplinary Policy and may, if the Headteacher considers it appropriate, be reported to the police.

Breaches of this Internet Access Policy by contractors or service providers will result in immediate termination of contract and may, if the Headteacher considers it necessary, be reported to the police.

Internet publishing statement

The School wishes for its web site to reflect the ethos, diversity of activities, individuals and education that can be found at the School. However, the School recognises the potential for abuse that material published on the internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the internet, staff should adhere to the following principles:

- Surnames of pupils must not be published
- No link should be made between an individual and any home address (including partial addresses or locations)
- Photos of pupils whose parents have opted out from publically displaying their child's photograph should not be used on the School website, newsletter or other publication
- Where there may be a child protection issue, no material should be published that could put the pupil at risk. In the case of a simple piece of artwork or writing, this may well be fine, but images should not be published. If in any doubt, refer to the School's Designated Safeguarding Lead (Isobel Boyt)

Use of portable equipment

The School provides portable computing equipment such as laptop computers, iPads and digital cameras to enhance the pupils' education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

Exactly the same principles of acceptable use apply as in the Acceptable Use Statement above.

Once equipment has been used, it should be returned to the resource area, put away in its correct order and put on charge, ready for future use.

If equipment such as iPads is taken offsite for use by staff in accordance with the Acceptable Use Policy and Internet Access Policy, the member of staff will bear responsibility if equipment lost or damaged.

Any costs generated by the user at home, such as iTunes, are the responsibility of the user.

Where a member of staff is likely to be away from School through illness, professional development (such as training, secondment etc.,) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to School. In the event of illness, it is up to the School to collect the equipment if the individual is unable to return it.

If an individual leaves the employment of the School, any equipment, including School encrypted USB sticks, must be returned before or on their last day of employment.

Pupils should not bring in their own USB sticks to load data onto the School computer system. Any work pupils wish to present via a computer must be emailed to their year group folder, their own email address or through the School Office so that it is virus checked.

No software, whether licensed or not, may be installed on computers in the care of staff as the School does not own or control the licences for such software.

Retention of digital data

All members of the School community must be aware that all emails sent or received on School systems, including deleted emails, are retained indefinitely. Email accounts are closed when that person leaves the School but the contents are retained indefinitely.

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g. for a reason set out in the School Privacy Notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. It is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

Breach reporting

Data protection law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- Loss of an unencrypted laptop, USB stick or a physical file containing personal data
- Any external hacking of the School's systems, e.g. through the use of malware;
- Application of the wrong privacy settings to online systems
- Misdirected post or email
- Failing to bcc recipients of a mass email
- Unsecure disposal

The School must generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, data controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. The School uses the GDPRiS platform to ensure compliance with this requirement.

If any member of the School community (including pupils where age appropriate) becomes aware of a suspected breach, they should notify the Bursar, who is responsible for data protection compliance within the School.

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all members of the School community. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Linked Policies

- Anti-bullying Policy for Pupils
- Anti-bullying Policy for Staff
- Behaviour Policy
- Curriculum Policy
- Online Safety Policy
- Prevent Policy
- Privacy Notice
- PSHCE Policy
- Safeguarding and Child Protection Policy
- Social Media Policy
- Staff Code of Conduct
- Taking, Storing and Using Images of Pupils Policy

THE CAVENDISH SCHOOL

Key Stage 1: Computer Studies Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to in school and at home	
2. I **CHECK** before I use new sites, games or apps with a trusted adult	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say they are	
6. I don't keep **SECRETS** just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared, just not sure or if I have made a mistake	

My trusted adults are:

_____ at School and

_____ at home

My name is _____

Parent signature _____

THE CAVENDISH SCHOOL

Key Stage 2: Computer Studies Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the School's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to. If I make a mistake I know that I can tell a trusted adult.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.

- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Pupil signature _____ Date _____

Parent signature _____ Date _____