GLENWOOD SECONDARY SCHOOL, EMSWORTH

CURRICULUM POLICY: COMPUTING

Reviewed	**September 2017**
Responsibility to Review	**Mark Pratley**
Next Review	**September 2019**

This policy should be read in conjunction with other policies including Online Safety, Social Use of Media, Anti-Bullying, Behaviour, PSHE, Data Protection and Freedom of Information and Assessment, Recording and Reporting policies.

With acknowledgment to St John the Baptist School, Southampton, Hampshire

STATEMENT OF INTENT

This policy aims to cover the different elements that Computing covers within our school, and to take account of recent developments in the curriculum with the introduction of the Computing curriculum to replace the Information and Communication Technology curriculum. These guidelines have been drawn up to ensure that all members of Glenwood School, both pupils and staff are aware of what is expected of them 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 enable these to go ahead. It sets out a framework for how Computing will be taught, assessed and monitored throughout the school and reflects the ethos and philosophy of the school. This policy aims to meet the criteria established by organisations such as Becta, 360^{o} Safe and ICT Mark.

Aims/Rationale

Computing comprises of there strands: Digital Literacy, Computer Science and, Information Technology. Computing encompasses every part of modern life and it is important that our pupils are taught not just how to use these tools but more importantly, how to use them safely. It is also important that our pupils have the confidence and ability to use these tools to prepare them for an ever-changing world. Staff, too, need to be confident and competent users of resources. We aim:

- To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use ICT to help improve standards in all subjects across the curriculum
- To develop the competence and skills of pupils through discrete lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure pupils 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 ICT to its full potential in all aspects of school life
- To use ICT as a form of communication with parents, pupils and the wider community

Curriculum

Computing is taught across the curriculum and wherever possible, integrated into other subjects. There is a need for Computing to be taught as a discrete subject to teach skills that can then be applied in other subjects as well as allow pupils to work towards accreditation. The long term Computing scheme of work shows the journey the pupils are expected to take but this will be adapted each year to ensure that it is relevant and up-to-date.

The Computing Coordinator ensures that the plans provide coverage of the National Curriculum Computing Programmes of Study and that pupils are both challenged and able to succeed. The scheme of work will show the move from the traditional ICT curriculum to the new Computing curriculum.

Online Learning / Learning at Home

As a school, we value the importance of providing opportunities for pupils to learn outside of school and we are planning to provide links to appropriate sites that pupils can access for further study.

Monitoring, Assessment, Recording and Reporting

i. *Monitoring:* Monitoring pupils' work is on-going via teacher observation and pupils' self-evaluation.

ii. *Assessment:* Computing is assessed in a number of ways using formative and summative assessment. Formative assessment occurs during Computing lessons, is conducted by the teacher on an informal basis and is used to inform future planning. Summative assessment tasks are provided at the end of each project. All pupils in Year 9 and 10 follow the OCR Entry Level Certificate in Information and Communication Technology syllabus with a view to having their coursework entered for assessment in Year 10. Pupils who choose the Computing option in Year 9 – 11 complete the syllabus with a view to having their coursework entered for assessment in Year 11.

iii. *Recording:* Recording pupils' progress is via Classroom Monitor, an online whole-school recording app. Work is marked in line with the Marking Policy and is monitored by regular 'Work Scrutiny' exercises undertaken by SLT.

iv. *Reporting*: Reporting pupils' progress to parents occurs formally during the summer term via the end of year reports with additional opportunities at the termly open evenings and, at mutually convenient times during the year if requested by a parent.

Opportunities and Inclusion

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

Roles and Responsibilities - The School

As a school we endeavour to ensure that parents and pupils are fully aware of ways in which the internet and ICT can be used productively and safely. We will always ensure that we provide pupils with the opportunities to excel and achieve when using ICT and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the pupils' safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters. A range of e-safety websites is provided on the school website as well as free copies of Vodafone's Digital Parenting magazine are distributed on a termly basis.

Roles and Responsibilities - Computing Coordinator

The Computing Coordinator will:

- plan and deliver a Scheme of Work, including provide assessment opportunities for all pupils
- inform staff of new developments and initiatives and provide training where appropriate.

- maintain an up-to-date hardware inventory and ensure the school has the appropriate number of software licenses for all software within the school.
- manage equipment and provide guidance for future purchasing.
- ensure procedures are sustainable
- oversee any external suppliers or contracts

Roles and Responsibilities – Staff

All staff sign the Acceptable Use Agreement (AUA) and report any online safety or cyber bullying issues that they encounter within or out of school in accordance with our online-safety procedures as listed below to the Designated Safeguarding Lead. All teachers and some LSAs have the loan of a laptop. It is the responsibility of staff to ensure that the internet security software and Windows Updates are regularly reviewed.

Roles and Responsibilities - Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers / other equipment within school that they are doing so appropriately. If either a visitor or governor wishes to have an account to logon to the school network, they should request this from the Computing co-ordinator. Users will also sign an AUA.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUA. They should ensure that they use the computers and equipment appropriately at all times and report anything that concerns them.

It is expected that pupils will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the pupils 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 child is accessing. They should also try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's tutor, the Computing coordinator or the head teacher / deputy Headteacher.

Passwords – Linked to 360^{o} Safe Password Guidelines

Staff only use passwords that are 'strong'; i.e. contain a mixture of some of the following; upper- and lower-case letters, numbers and special characters. The password policy on the network forces staff to regularly change their network and email passwords.

Pupils will be taught about 'strong' passwords and encouraged to use a strong password if they are capable of doing so.

Backups

The data stored on the school's network is backed up and securely stored by an external company approved by the Governors. (Coretek)

School Website

The school website is overseen by the Computing co-ordinator - but managed by Coretek. The Computing co-ordinator ensures the website is informative, up to date and meets the requirements for Ofsted.

Internet and E-mail

The internet may be accessed by staff and by pupils throughout their hours in school. We ask as a school that staff are vigilant as to the sites pupils are accessing and pupils should not be using the internet unattended. All PCs face outwards so their screen is visible from any point in the room. Where pupils are using laptops, staff need to be extra vigilant as the screens are not so easily monitored.

The teaching of email and internet use and online safety are be covered within the Computing curriculum, although staff also encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All members of staff are issued with a school email address and this is the email with which they should use for professional communication. Staff should take extra care to ensure that all communication with or parents remains professional. Staff do not contact pupils via email. Users are responsible for all messages that are sent and due regard is paid to the content of the emails to ensure cannot be misconstrued. Currently, pupils are only issued with an email address when the curriculum requires it.

The internet and filtering is provided by Hampshire County Council. All Computing activity, including internet use is monitored the Securus server which identifies the device, either PC or laptop with the location, the time and the user. Many inappropriate websites are filtered out by the local authority and the Securus server can be configured to filter additional sites although this is not 100% effective therefore the need for staff vigilance.

Personal Data

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information on to personal devices unless strictly necessary and only with the permission of the Headteacher or Deputy Headteacher. This data should then be removed as soon as possible. When using a personal laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display.

Social Media - Linked to 360° Safe 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. We will ensure that staff and pupils 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 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 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
- 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 pupils

Younger pupils should not be signed up to most social networking sites due to the over-13 age limit, an Act of United States Law, The Children's Online Privacy Protection Act which prevents websites collecting data or providing their services to users under the age of 13. 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 pupils are using these sites.

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

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

- Will ensure that their parents or guardians have given us written permission
- If we do not have permission to use the image of a particular pupil, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily

- Will ensure that pupils are in appropriate dress and we do not include images of pupils who are taking part in swimming activities
- Ask that if a parent, guardian or pupil wishes, they can request that a photograph is removed from the website. This request can be made verbally or in writing. We will endeavour to remove the image as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Ask parents to sign an agreement form to indicate the degree of publication / distribution of images.
- Staff should not use their personal cameras or phones to take photographs of pupils but if it is unavoidable, the images must be deleted as soon as possible afterwards.

E-Safety – Linked to 360° Safe E-Safety Guidelines

At Glenwood School we take online safety very seriously. We ensure that it is taught throughout the ICT curriculum and highlight instances when it occurs in the news. We also provide pupils with dedicated online safety lessons each term. These will be reviewed regularly to ensure that they are up-to-date and reflect current needs. Pupils are taught how to act online and how to minimise the risk when working on the internet. Pupils are taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

If a member of staff suspects an online safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. Depending on the incident it should be reported to a Designated Safeguarding Lead or Computing ICT Coordinator for further action.

The use of the internet to access inappropriate materials such as auction sites, gambling sites, pornography, racist or any other material is prohibited. If users do see an inappropriate website or image, they must inform the member of staff taking the lesson who complete and E-safety Record Sheet and hand to a Designated Safeguarding Lead.

If pupils receive an email that they believe to be inappropriate then they must show it to the member of staff and/or the Computing co-ordinator who will investigate.

Complaints

Incidents regarding the misuse of the Internet by students will be delegated to the ICT Coordinator who will decide which additional evidence should be gathered or recorded. The Securus server will be crucial in providing a record of an incident / evidence. A partnership approach with parents is encouraged. Any complaint about staff misuse will be referred to the head teacher. Complaints of a child protection nature must be dealt with in accordance with the Child Protection Policy.

Copyright and Intellectual Property Right (IPR)

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.

Pupils will have discussions about the proper use of images with questions such as 'Is it OK to use an image we find online?' and for pupils 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 Hampshire County Council.

Technical Support

Many minor issues are dealt with buy the Computing co-ordinator with more technical support provided remotely or on site by Coretek. Additional office-based support is provided by the Hampshire IT helpdesk and forms part of the Service Level Agreement.

Sustainability, the Environment and Planning for the Future

To ensure the level of Computing across the school is sustainable, the Computing co-ordinator is responsible for maintaining an inventory of assets with a view to a planned programme of replacement / upgrade. The Computing budget is set annually by the Governing Body although money can be put aside for a longer term project such as replacing whiteboards with interactive screens and is allocated to be spent in a later financial year. Where possible, hardware will be recycled, either to a local school or an approved recycling contractor, providing data protection is not compromised.