West Walker Primary School
Computing Policy 2019-2020

Curriculum

Computing skills will be taught in discrete sessions and then applied across the curriculum. Children will be taught using PCs and iPads. Year groups plan using the National Curriculum (2014) or Early Years Curriculum. Moderation ensures that children are challenged and able to succeed. As a school, we value the importance of providing opportunities for children to learn outside the classroom and our website provides links to appropriate websites. Children's progress will be assessed using GEM Education computing assessment grid alongside the curriculum programme of study. All pupils are provided with opportunities to access the computing curriculum and where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all children to achieve.

The Senior Leadership Team and Subject Coordinator:

- Decide on the provision and allocation of resources, in accordance to the school development plan, computing action plans and timescales.
- Oversee planning, teaching and assessment to raise standards.
- Responsible for staff development and providing training where appropriate.
- Ensure all the resources are kept up to date (software and hardware) and provide guidance for future purchasing.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the Senior Leadership Team. Memory sticks will be scanned by the school's antivirus software. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP. The installation of software unauthorised by the school, whether licensed or not, is forbidden. The school reserves the right to examine or delete any files that are held on its system.

Laptops

- Staff provided with a laptop purchased by the school can only use it for private purposes at the discretion of the Headteacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the Computing subject leader
- Laptops belonging to the school must have updated antivirus software installed and be password protected
- Staff intending to bring personal laptops on to the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop
- Staff should not attach personal laptops to the school network
- The security of school laptops is of prime importance due to their portable nature and them being susceptible to theft
- See School Laptop policy (Appendix IV of the WWPS E-Safety Policy)

iPads
Staff are responsible for the school iPads designated to their year group. Staff are not permitted to install any apps on the school iPads without permission from the Senior Leadership Team or ICT Manager.
Children should be reminded of the e-safety policy and Acceptable Usage Policy whenever they use iPads.

Network
Staff will be issued with a username for the computer consisting of their payroll number and a password. It is their responsibility to change this in accordance with the password procedure below. Pupils in Early Years and KS1 will be expected to use a generic class login and password. All KS2 children will be assigned an individual login. These accounts will be created and monitored by a NEAT Computing Technician.

School Website
The school website will be overseen by the subject coordinator and ICT Manager. Statutory guidance will be cross referenced whilst updating the website. It is expected that certain content will be provided by members of staff when necessary.

Internet and E-mail
All staff and children must refer to the e-safety and acceptable usage policy when accessing the internet and email. All members of staff will be issued with a school email address; (forename.surname@westwalker.newcastle.sch.uk). This is the email with which they should use for professional communication. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. The internet and filtering is provided by the local authority, who run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by the local authority. Additional sites can be enabled or disabled by the Senior Leadership Team or ICT Manager and a record is available from the Local Authority upon request.

Passwords –Password Guidelines
Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation.

School Liaison, Transfer and Transition
When a new account is needed (child and staff) it is the responsibility of the Senior Leadership Team to inform the Local Authority for a network login to be created. If a person leaves the account and content will be removed.

Age Limits
Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.
As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will also post details of these sites on our school webpage. Occasionally these sites will be used by teachers with a class, for example to create a class book or movie, but not by a child with their own personal account. We will make parents aware of this during our e-safety events.

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

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand

that some staff members have friends within the local community (such as children's parents) and just ask that these members of staff take extra precaution when posting online
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- 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 work based incidents or individuals.
- Check with the Subject Coordinator if they need advice on monitoring their online persona and checking their security settings

As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.

As a school we will use Twitter and Facebook to post information, updates and blog posts. Photos will only be used where a parent has given permission. These may stream directly to our school website. We will ensure that we block any followers that appear inappropriate. We will follow guidance laid out in this document to ensure children are kept safe. Spam messages (often containing inappropriate links and language) are caught by software installed on the blog (akismet) and this is monitored by the subject coordinator. This is also updated regularly.

Digital and Video Images

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

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

Technical Support

Any issues must be logged on the ICT Issues drive; this is the staff's responsibility. These will then be dealt with by the ICT Technician, Subject Coordinator or the Digital Leaders as appropriate. Outcomes will be recorded next to the issue.

Additional office-based support (e.g. MIS, SIMs) is provided by the Newcastle City IT Helpdesk and forms part of the annual Service Level Agreement that the school has in place.

Sustainability and Environmental Impact

To ensure that the level of Computing across the school is sustainable, the subject coordinator is responsible for the upkeep of the electronic Computing Handbook which will contain usernames, passwords and guides to online tools and software as well as details of licenses and a complete Inventory. Hardware is disposed of safely and securely through a local company approved by NEAT.