Downlands ICT Policy

This policy has been written taking advice from many different local authorities and other schools.

This policy should be read in conjunction with other policies including Mobile Technologies (see appendix) Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection, Copyright Protection and Freedom of Information policies.

Introduction

This policy aims to cover the different elements that Information Communication Technology (ICT) can cover within our school. 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 enable these to go ahead. This policy will set out a framework for how ICT 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 Becta, 360Safe and ICT Mark. Often schools will have a number of policies including E-safety and Social Media, but as a school we have decided to combine them into one policy.

Aims/Rationale

ICT 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 independent users and learners of ICT 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 computing competence and skills of pupils through computing 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 and are provided with exciting, creative ways in which to share their learning
- To use tools 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 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

ICT will be taught across the curriculum and wherever possible, integrated into other subjects. There may be a need for stand-alone ICT sessions to teach skills that can then be applied in the cross-curricular sessions. Children may be taught ICT using the iPads and computers. The long term ICT map will show the journey in which the children are expected to take but this will be adapted each year to ensure that it is relevant and up-to-date.

The ICT Coordinator will ensure that the plans provide coverage of the National Curriculum Programmes of Study and that children are challenged and are able to succeed.

In Reception, children will be taught how to use various pieces of ICT equipment, including the computers, in accordance to the Early Learning Goals appropriate for them.

Online Learning

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

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

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

- Provide links to websites suited to the current topic
- Provide logins for online tools such as Education City and IXL

For Key Stage 2 children, we will also:

- Provide a personal login for their portfolio site.

Assessment

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during Computing lessons and will be used to inform future planning and this is conducted by the teacher on an informal basis. Computing capability will be completed on a termly basis with notes being taken by the teacher and this will link to the school's Assessment framework which in turn relates to county assessment strategies and National Curriculum levels.

Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the ICT 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 - Senior Management Team

The head teacher and other members of the senior management team are responsible for monitoring the teaching of Computing throughout the school. They will also oversee the completion of the Self-Review Framework and 360Safe E-Safety Framework. The senior management team should decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, Computing action plans and timescales. They should also ensure that the ICT subject leader and teachers are following their roles as listed below and in accordance to job specifications and performance management targets.

Roles and Responsibilities – Computing Subject Leader

The Computing Subject Leader will oversee planning in all year groups throughout the school and be responsible for raising standards in Computing. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The Computing Subject Leader is responsible for overseeing the assessment of ICT across the school and providing opportunities to moderate Computing ability. They are responsible for keeping the hardware inventory up-to-date and ensuring the school has the appropriate number, and level, of software licenses for all software within the school. The Computing Subject Leader is responsible for managing equipment and providing guidance for future purchasing. The ICT Subject Leader is also responsible for ensuring tools and procedures are sustainable.

Roles and Responsibilities - Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach Computing and to use Computing within their class. This will be in accordance to the schemes of work provided by the Computing Subject Leader. They will also assist in the monitoring and recording of pupil progress in Computing. Teachers should also respond to, and report, and e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below.

Whilst checking of personal sites, e.g. email, is permitted during non-contact times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and ensure they are logged off appropriately. Staff should follow, and agree to, the Acceptable Usage Policy below.

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 and equipment within school that they are doing so safely. If either a visitor or governor wishes to have an account to logon to the school network, they should speak to a member of the senior management team.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and ICT can be used productively and safely. We will always ensure that we provide children 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 children's safety is at the forefront of our thoughts and we will keep

parents informed as necessary through newsletters and parents events. A range of e-safety websites, and our e-safety planning, will be made available on the school website.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities - Parents

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

Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher and/or ICT coordinator. If staff use memory sticks then the school's antivirus software will scan these. 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. If you are unsure, please speak to the head teacher and/or the ICT Coordinator for advice. The school reserves the right to examine or delete any files that are held on its system.

Backups

The data stored on the school's network is scheduled to backup on-site each week. This will allow backups of files to be recovered if the original becomes lost or damaged.

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

The school website will be overseen by the ICT Subject Leader and it is expected that certain pages will be updated by other members of staff and children. The blogs use a Wordpress installation.

Google Apps

The school's online learning space will be a system based around Google Apps for Education and personal portfolios. All children will be given a login and will be given permission to use different tools according to their age and e-safety awareness.

Google stores data about its users in accordance with the Safe Harbour Agreement approved by Becta before its closure in 2011.

Internet and E-mail

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

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

All members of staff will be issued with a school email address and this is the email with which they should use for professional communication. Children will also be issued with an email address on entering Key Stage 2 and this should be monitored by the class teacher and the ICT coordinator. Staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the ICT coordinator so it is the user's responsibility to ensure they log off appropriately.

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

The internet and filtering is provided by SWGFL and the ICT coordinator will run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by the local authority. The local authority provides three ports through which to connect to the internet.

Passwords – Linked to 360Safe Password Guidelines
Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.
For online services used in school such as blogs, Twitter , Viddler, Wallwisher and Animoto, there is an account per class and a password across the school. It is important that these details are not given to pupils at any point.
School Liaison, Transfer and Transition
When a new child joins, it is the responsibility of office staff to inform the ICT coordinator of the child's name and year group. The ICT coordinator will then provide a network login and
At the end of a child's time with us, they will be able to take their schoolwork with them should they wish. Photographs will be checked to ensure we have permission to share them before this takes place.
Where a new school is known a user name and password will be sent to the new school, to enable them to see the child's work.
Mobile Phones and Handheld Devices – Linked to 360Safe Mobile Phone Guidelines – See Appendix 1
Staff may attempt to connect their phone to the school's wireless network in accordance with the network guidelines.
Age Limits
Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.
As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will also post details of these sites on our school webpage. We will ensure that these will tend to be sites that allow creation of content rather than searching other users' content.
Occasionally these sites will be used by teachers with a class, for example to create a class book or movie, but not by a child with their own personal account. We will make parents aware of this during our e-safety events. If they do not wish their child to access these sites, their child can be provided with an alternative method to complete the task.

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. 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 360Safe Social Media Guidelines
As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.
Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils 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 children

- Check with the ICT Subject Leader if they need advice on monitoring their online personal and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur. As a school we will use Twitter to post information, updates and blog posts. These will stream directly to our school website. We will ensure that we block any followers that appear inappropriate.
We will use blogging throughout the school to share children's learning and to communicate with parents. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post on the blog or write a comment without it being approved by a teacher to ensure that the children are not subjected to any inappropriate comments. Spam messages (often containing inappropriate links and language) are caught by software installed on the blog (akismet) and this is monitored by the ICT Subject Leader. This is also updated regularly.

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

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

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

If staff use personal cameras or phones to take photographs of children within school, these should be removed from the device as soon as possible. We are fully aware that this is necessary at times, but precautions should be taken to minimise the risks.

Sustainability and Environmental Impact – Linked to ICT Mark 1b4

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

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

At Downlands we take E-safety very seriously. We will ensure that it is taught often throughout the children's ICT and PSHE sessions as necessary. We will also provide children with dedicated e-safety lessons per term. Links to E safety resources will be available on the school website for parents to view. These will be reviewed regularly to ensure that they are

up-to-date and reflect current needs. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them. Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual e-safety focussed parent meeting and will provide regular updates via our website and newsletters as appropriate.
All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the school. All staff will also complete an AUP.
E-safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online.
If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the ICT Coordinator and head teacher and recorded as appropriate.
If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the ICT Coordinator 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. A partnership approach with parents will be 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 child protection procedures.

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

Responding to unacceptable use by staff
Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.
Responding to unacceptable use by pupils
Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

Reviewed June 17
Review Oct 19

APPENDIX 1

Mobile Technologies Policy (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils / students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices

for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	**No**	**Yes**	**No**
Full network access	*Yes*	*Yes*	*Yes*	No	Yes	
Internet only						
No network access						

- **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete / amend as appropriate):**
    - **All school devices are controlled though the use of Mobile Device Management software**
    - **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)**
    - **The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**

[1]Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

- **For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted**
- **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user**.
- *All school devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*

- *When personal devices are permitted:*
  - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
  - *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
  - *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
  - *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
  - *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
  - *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
- **Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;**
  - **Devices may not be used in tests or exams**
  - **Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements**
  - **Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
  - **Users are responsible for charging their own devices and for protecting and looking after their devices while in school**

- **Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day**
- **Devices must be in silent mode on the school site and on school buses**
- **School devices are provided to support learning. It is expected that pupils/students will bring devices to school as required.**
- **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
- **The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted**
- **The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps**
- **The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.**
- **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
- **Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
- **Devices may be used in lessons in accordance with teacher direction**
- **Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances**