Acceptable Use of ICT (Internet and Computer Technology)

Responsibility for Document:	Computing Leader/SLT
Approved Date:	Autumn 2019
Review Date:	Autumn 2021

This policy is to be read in conjunction with the Mission Statement, Teaching and Learning Policy, Positive Behaviour Policy, Anti-bullying Policy, Curriculum policy, Child Protection and Equality Policy, SEND policy, Computing Policy.

At Denmead Junior School, we strive to create a <u>growth mind-set for learning</u> and life for all our children by using growth mind-set language and behaviours. This encompasses all interactions, between pupils and staff, amongst staff and amongst pupils. In addition we promote the <u>Learning Powers</u> of <u>resilience, reflection, co-operation, concentration and curiosity</u>. In everything that we strive to do and the way that we do it, we promote, model and teach the children the <u>Values</u> of <u>Friendship, Understanding,</u> and PRIDE <u>(Positivity, Respect, Inspiration, Determination and Excellence).</u>

1. Aims

We are committed to using the internet and all it offers in the most effective and appropriate way at our school, for the benefit of our pupils, staff and community. To this end, we have developed this Acceptable Use of ICT policy, to ensure that all members of our school community understand what is expected of them when they use the internet, mobile communications, computer resources, intranet and virtual learning environment, e-mails, social networking sites, instant messaging services and camera and recording equipment.

2. Objectives

The purpose of this policy is to enable children, family and employees of Denmead Junior School to

- gain maximum benefit from ICT resources
- to protect children, staff and the school from any liabilities
- communicate to all users how they <u>should</u> and <u>should not</u> use ICT facilities

whether it is using the school's or personal equipment.

3. Roles and Responsibilities

Members of the school community have different roles and responsibilities when it comes to using the Internet at school.

Role	Responsibilities regarding Internet Use in school
Head Teacher	To monitor this Policy and ensure it is updated yearly and agreed with all staff.
Senior Leadership Team	To ensure that the Policy is implemented in all phases of the school.
Head Teacher	To ensure that the school website is kept up-to-date and follows appropriate guidelines.
Computing Leader	To develop the use of the Internet as a teaching and learning tool across the school. To keep up to date with developments in Internet issues as they relate to education, and keep

	staff informed.
School Administration Manager	To ensure that appropriate filters are maintained on the network and issues of inappropriate access reported to the ICT helpdesk.
Class teacher/Subject Teacher	To ensure that pupils use the Internet purposefully and with adult supervision at all times. To know how to deal with incidents involving unsuitable material or situations where pupils feel uncertain or unsafe when using the Internet at school. To understand this policy and abide by the rules for staff.
Governing Body	To check that this policy is up to date and reviewed every 2 years.
Pupils	To abide by the rules of this policy for children.
Parents and Carers	To support their child to abide by the rules of this policy
Other Community Users	To agree to follow this policy when using school facilities under extended service agreements

4. Access

The school, in conjunction with Hampshire County Council provides a suitable Internet connection, with broadband capabilities. All areas of the school are connected to the Internet through both wired and wireless connections.

The school uses the standard LA Internet Service Provider through Hampshire ICT. The school is connected through HPSN2 which is a high quality and resilient fibre-optic network.

The following have access to the Internet at school:

- All staff members of Denmead Junior School will have access to a school owned computer/laptop.
- All visitors/guests of Denmead Junior who may be connecting to the school network either via school equipment or their own personal equipment.
- All third parties or suppliers who may also remotely access any school equipment in the course of their work with the school.
- All pupils have access to the Internet as part of the curriculum.
- Computing clubs and after school provision. (The school may run computing and home learning clubs at lunchtimes and after school led by a member of the school staff.)
- Extended Services, (As part of their agreement with the school, services may have access to the school's internet – e.g. Denmead Day Care which provides before and after school care using the school's premises.)
- Parental Access. (If parents do not have access to the internet at home and need to in order to fill in various school forms e.g. admission to secondary schools they can do at school with a member of our administration team.)

5. Security and Confidentiality

Any concerns about the security of the ICT system should be raised immediately with a member of the senior leadership team.   Staff who abuse this policy may be subject to the school's disciplinary procedures.

Staff emails to and from the school can and will be monitored for inappropriate use along with internet access within the school.

All internet sites accessed by the user are logged with date and time of access. Staff must not use school resources to access social networking sites, with the exception of approved office staff. Most social networking sites are banned on the schools internet sites however these can be accessed via the WIFI access in the school on personal mobile phones (please see the Computing Leader for details).

Staff and those who have line management responsibility are advised to consider the appropriateness of accepting colleagues, particularly those who they manage, as friends on social networking sites.

Security and virus protection

The school subscribes to the LA Antivirus software program, which uses McAfee Antivirus software. The software is updated regularly and automatically through the network and by our external technical support staff.

Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the Senior Leadership Team.

Content filter

Hampshire schools use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.
Pupils and staff are not allowed to download any programmes that may affect the performance of a machine without first consulting the Computing Leader.

Portable storage devices and CD-ROMs etc

Portable media such as CD-ROMs and personal hard drive devices are a common way of introducing a virus or other undesirable agent into a school computer system. Staff should minimise their use of these and only use devices which are encrypted and supplied by the school. Staff should take care that files from other computers outside the school are checked for virus contamination before they are used on the school system.

Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous.

Legal issues

Our school is aware of the data protection law as it affects our use of the internet, both in administration and teaching and learning. We adhere to the LA Guidelines on Data protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes. Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the internet by members of the school community using the connection provided by the school.

6. Using the internet with pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and the internet is an integral part of that world. At our school we are committed to teaching pupils to use the internet effectively, appropriately and safely in all aspects of their education.

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. We teach all of our pupils how to find appropriate information on the internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

• Teachers carefully plan all internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
• Children are taught how to use search engines and how to evaluate Internet-based information as part of the computing curriculum and in other curriculum areas where necessary.
• They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
• They are taught how to carry out simple checks for bias and misinformation.
• They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

For pupils internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always supervised by an adult when using the internet.

Breaktimes

At breaktimes children are not allowed to access computers. If they have been asked to complete a computer related task then this is done with a member of staff supervising.

Parents' Evenings and before/after school meetings

Children who attend with their parents are therefore their parent's responsibility. They should not access school computers during these times.

Teaching safe use of the Internet

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use our Personal Development Learning (PDL) in conjunction with our Computing lessons to teach children how to use the internet safely. Children are taught in Year 3 how to complete safe searches on the internet, what to do if they find inappropriate material and who to report it to. In Year 4, they learn about wider services available on the internet and how to use them safely. In Year 5 and 6, children learn about acceptable and unacceptable behaviour when using online services and technologies and the importance of password security. This learning is continually renewed through the school year.

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than ban internet use apart from strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at home.

Unsuitable material

Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the Administration Manager and Head Teacher.
3. Logging the incident.

4. Informing the LA/Internet Service Provider so that the website can be added to the content filter if appropriate.

5. Discussion with the pupil about the incident, and how they might avoid similar experiences in future.

6. Informing parents and carers

Deliberate misuse of Internet facilities

All pupils must follow the DJS Charter of Good Online Behaviour and Use of ICT. The class teacher will explain this carefully to all pupils before they sign it. (See Appendix 3)

Where a pupil is found to be using the internet and ICT resources inappropriately the following sanctions will apply:

❖ For viewing unsuitable material (e.g. violent games, unsuitable celebrity pictures, music downloads, redtop news websites etc that have somehow got through the school's online security); accessing chat rooms; sending unacceptable messages; deliberately changing screensavers and passwords and for using the classroom computer linked to the Interactive Whiteboard without permission:

Sanctions will include:

Initial warning from class teacher
Loss of playtime
Apologies to offended pupils/adults
Reduced access to internet for one or more lessons
Letter/phone call to parent/carer
Report to Head Teacher

❖ For accessing offensive material (e.g. pornographic images, racist, sexist or hate website or images that have somehow got through the school's online security); sending offensive messages:

Sanctions will include:

Incident logged with the Designated Safeguarding Leader and reported to Head Teacher
Head Teacher meeting with parent/carer
Removal of Internet privileges/username etc
Loss of playtimes and other school privileges
Internal or external exclusion
Police involvement

❖ For incidences that occur outside school between children, but the effects of such behaviour come into school, the school will work with parents and carers to educate and sanction as appropriate.

The school website and blogging

Any photo uploaded to the website must have parental permission. The website will not disclose personal information about staff including their photographs. The website will contain access to school blogs and these have their own online security measures (see below).

As part of the Computing Curriculum, children may learn to set up and publish their own blogs. Material will only be published once it has been checked by the class teacher or member of school staff. Similarly children's comments on other children's blogs can only be published once they have been approved by the class teacher or school staff member.

E-Mail/Messaging systems

We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively. We teach the use of e-mail and other online communication services (such as Skype) as part of our Computing curriculum, and use it across the curriculum in a range of ways.

Pupils are not allowed to access personal e-mail using school internet facilities, due to the quantity of unsolicited e-mail (spam), unsuitable content and virus threats associated with commercial e-mail accounts.

Chat and online discussion/newsgroups, online gaming, instant photographs and messaging through a range of hardware (phones, tablets, X-box, apps etc) are discussed throughout our PDL and Computing curriculums and all reported incidents of their misuse that can occur outside of school are addressed by staff in the manner mentioned in this policy.

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas. This area of technology is growing so fast that new ways of instant messaging are continually being created.

All of these present a range of personal safety and privacy issues for young people, including the rise of cyber-bullying.

We use the resources, guidelines and materials linked to the National Curriculum to teach children how to use all these communication methods safely.

School Learning Platform

At present the school does not operate one of these, but we are looking to develop resources and materials that can be accessed from pupil's homes. Presently children can access Times Table Rockstars and more are being considered as the year progresses. Children have their own logins.

7. Whistleblowing and Cyberbullying

The school will not tolerate any form of bullying including electronic online bullying.

The misuse of email/messaging systems or the internet for harassing people such as sending unpleasant or aggressive messages/photographs is unacceptable. The school has the right to monitor all internet and email/messaging activity within bounds in order to keep the internet safe for all at Denmead Junior School and to protect from online bullying. Our internet activities therefore are filtered and websites blocked for safety.

Staffs who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Head Teacher to such abuse.

Where a concern relates to the Head Teacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Officer.

It is recognised that increased use of ICT has led to cyber bullying and/or concerns regarding e-safety of school staff.

Staff are strongly advised to notify their Head Teacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available age 9 of 17 through Hampshire's Confidential Counselling Service, Employee Support Line (02380 626606) and also via the UK Safer Internet Centre helpline@safetinternet.org.uk or 0844 381 4772.

Online bullying and harassment

Online bullying and harassment via Instant messaging, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. Please also refer to the school's Anti-Bullying Policy.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

8. Safe use of images and videos

Digital images and videos are easy to capture, reproduce and publish and, therefore, misuse.

We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips. Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Head Teacher.

Images and videos of pupils will be stored on the school's network only. Staff and pupils are not permitted to have images or videos on personal portable media. Right of access will be restricted to the teaching staff and pupils within the confines of the school network.

Parents are permitted to take images or videos for personal use only. Pupils and parents are not permitted to put any images or videos online of pupils, other than their own children, via social networking sites or other websites.

Any photos or videos taken on a school trip belong to Denmead Junior School and must be uploaded onto the school network on the same day and deleted from any personal devices. If parent helpers have taken photographs on behalf of the school these must also be uploaded onto the school network on the same day and deleted from the portable device.

Children will be taught about appropriate use of images when using digital equipment and mobile phones.

9.   Monitoring

This policy will be monitored by the SLT every two years. The policy may be reviewed more frequently that this in order to keep up with the advances in on-line technology.

Internet history searches will be monitored periodically by the computing lead, senior leadership team and chair of governors. Internet search histories will be checked through the Hampshire Schools Services provided by Hampshire. Results can only be accessed by the computing leader, Designated Safeguarding leader and Chair of Governors.

 Monitoring checks will be regularly carried out half termly, with additional checks carried out if warranted by additional circumstances e.g unacceptable use seen by staff members, other child reports or other information gained. Monitoring checks will be monitored by the Designated Safeguarding Leader.

Appendix 1:

Use of ICT Resources Do's and Don'ts: Advice for School Staff

General Issues

Do	Don't
- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources - ensure that where a password is required for access to a system, that it is not inappropriately disclosed - respect copyright and intellectual property rights - ensure that you have approval for any personal use of the school's ICT resources and facilities - be aware that the school's systems will be monitored and recorded to ensure policy compliance - ensure you comply with the requirements of the Data Protection Act when using personal data - seek approval before taking personal data off of the school site - ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely - report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Head Teacher or designated manager and/or Child Protection Liaison Officer as appropriate - be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal - ensure that any equipment provided for use at home is not accessed by anyone not approved to use it - ensure that you have received adequate training in ICT - ensure that your use of ICT bears due regard to your personal health and safety and that of others - Restrict the use of unsecure portable storage devices for school and use remote access where ever possible. Use encrypted storage devices from the school if needed. - Ensure that your computer is locked when leaving it at breaktime, lunchtime and at other periods when you are away from it.	- access or use any systems, resources or equipment without being sure that you have permission to do so - access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for - compromise any confidentiality requirements in relation to material and resources accessed through ICT systems - use systems, resources or equipment for personal use without having approval to do so - use other people's log on and password details to access school systems and resources - download, upload or install any hardware or software without approval - use unsecure removable storage devices to store personal data - use school systems for personal financial gain, gambling, political activity or advertising - communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of email, the internet, VLEs and school and HCC intranets

Do	Don't
- alert your Head Teacher or designated manager if you receive inappropriate content via email - be aware that the school's email system will be monitored and recorded to ensure policy compliance	- communicate with pupils or parents from your personal accounts. - send via email or download from email, any inappropriate content

▪ ensure that your email communications are compatible with your professional role ▪ be aware that the school may intercept emails where it believes that there is inappropriate use ▪ seek support to block spam ▪ alert your Head Teacher or designated manager if you accidentally access a website with inappropriate content ▪ be aware that a website log is recorded by the school and will be monitored to ensure policy compliance ▪ answer email messages from parents via the school's account within your directed time ▪ Use your school email for all work related matters and your personal email for personal matters ▪ Only access your personal emails during school break times	▪ send messages that could be misinterpreted or misunderstood ▪ use personal email addresses to communicate with pupils or parents ▪ send messages in the heat of the moment ▪ send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude ▪ use email systems to communicate with parents or pupils unless approved to do so ▪ download attachments from emails without being sure of the security and content of the attachment ▪ forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention ▪ access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet ▪ upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do	Don't
▪ ensure that your communications are compatible with your professional role ▪ access your mobile phone only at break times, making calls in the PPA room ▪ ensure that you reimburse your school for personal telephone calls as required ▪ use school mobile telephones when on educational visits ▪ If, for some reason you have to use your phone to access school emails or school resources for teaching and there are children present tell them what you are doing so that they understand why you have your phone out ▪ Keep your phone in a secure place during the day	▪ Use your phone or look at it during lessons ▪ send messages that could be misinterpreted or misunderstood ▪ excessively use the school's telephone system for personal calls ▪ use personal or school mobile telephones when driving ▪ use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do	Don't
▪ ensure that material recorded is for educational purposes only ▪ ensure that where recording equipment is to be used, approval has been given to do so ▪ ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy	▪ bring personal cameras or recording equipment into school without the prior approval of the Head Teacher ▪ inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded ▪ put material onto the VLE, school intranet or intranet

- ensure that parental consent has been given before you take pictures of school pupils - Use school cameras at all times and download materials to the school system as soon as possible, deleting them from the camera at the same time - Give school cameras to parents who help on class trips and collect them in at the end of the day to download.	without prior agreement from a member of senior staff

Use of social networking sites

Do	Don't
▪ ensure that you understand how any site you use operates and therefore the risks associated with using the site ▪ familiarise yourself with the processes for reporting misuse of the site ▪ consider carefully who you accept as friends on a social networking site ▪ report to your Head Teacher any incidents where a pupil has sought to become your friend through a social networking site ▪ take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain ▪ ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page ▪ follow school procedures for contacting parents and/or pupils ▪ only contact pupils and/or parents via school based computer systems and telephones ▪ through your teaching, alert pupils to the risk of potential misuse of social networking sites ▪ Think very carefully about accepting friendship request from parents and ex-parents - you may be giving them access to personal information, and allowing them to contact you inappropriately ▪ Consider carefully the appropriateness of accepting colleagues, particularly those who they line manage, as friends on social networking sites	▪ access social networking sites while at work ▪ accept friendship requests from pupils or ex-pupils ▪ put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial ▪ post anything that may be interpreted as slanderous towards colleagues, pupils or parents ▪ use social networking sites to contact parents and/or pupils ▪ post a 'like' to the school's Facebook page. This will give facebook visitors access to your own page.

Appendix 2: Acceptable use of ICT policy 2019/2020

Staff Acceptable Use of ICT Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I understand that I must not use the school ICT system to access inappropriate content.

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that school information systems **and hardware** must not be used for private purposes without specific permission from the Head Teacher.

- I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.

- I will not install any software or hardware without permission.

- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must NOT be kept on removable storage devices *with identifiable personal information.*

- If I need to use a portable storage device, I will use a school one which will be encrypted, but wherever possible I will access the school system remotely when working away from the school site.

- I will respect copyright and intellectual property rights.

- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

- I will report any incidents of concern regarding children's safety to the Designated Child Protection Liaison Officer or Head Teacher.

- I will not accept friendships with pupils or ex-pupils on social networking sites.

- I understand that I am strongly advised not to accept friendships via social networking with parents, ex-parents and governors. If I do decide to accept such friendships, I must not engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT 2019/2020

Signed: ……………………………………………..   Date: …………………………………………

Print Name: …………………………………………….

Pupil's Acceptable Use of ICT Agreement

Appendix 3: Acceptable Use of ICT Policy 2019/2020

DJS Charter of Good Online Behaviour and Use of ICT

I understand that these rules are to keep everyone safe and to help us use the internet and other electronic devices sensibly and appropriately at school.

I promise:
- To only use the school ICT for educational purposes and to only access age appropriate websites.
- Not to look for or show other people things that may be upsetting.
- To show respect for the work that other people have done.

I will not:
- Look at or use other people's work or pictures without permission to do so.
- Damage the school's ICT equipment. If I accidentally damage something I will tell my teacher.
- Share my password with anybody. If I forget my password I will let my teacher know.
- Use other people's usernames or passwords.
- Share personal information online with anyone. I will not give my home address or telephone number or arrange to meet someone, unless my parent/carer gives permission.
- Download anything from the internet unless my teacher has asked to me to.
- Bring my mobile phone into school.
- Bring in any software, disks or memory sticks into school without permission.
- Change school passwords, screensavers or use computer that are connected to the Interactive White Board without permission

I will:
- Ask permission before using the Internet and only use it when a teacher or adult is with me.
- Let my teacher know immediately if anybody asks me for personal information.
- Let my teacher know immediately if anybody says or does anything to me that is hurtful or upsets me.
- Be respectful to everybody online. I will treat everybody the way that I want to be treated.
- Hand in any electronic device into the office for safekeeping, including my phone if I use one for safety reasons for my journey to and from school (permission forms must be completed by your parents)
-
- Send in any home learning via the email addresses set up for my year group.

I understand:
- That not everything on the internet is true and some people on the internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home.
- That I represent the school and that all communications sent by me will be polite and sensible.
- If I break the rules in this charter there will be consequences in line with the school's Behaviour Policy and my parents will be informed.
- That the school will check my computer files and will monitor the internet sites I visit.

Name	Year Group/Class	Teacher
Signed		Date

Appendix 4: Acceptable Use of ICT Policy 2019

Dear Parents and Carers,

<u>**Using the Internet at Denmead Junior School**</u>

At Denmead Junior School, we believe that the Internet is an essential part of your child's learning. It offers a huge range of useful and educational material and information and it is an important part of teaching and learning across the curriculum.

Our school provides Internet access to pupils, and we have clear rules and guidelines on how this access will be managed and made as safe as possible

We have taken positive steps to deal with the risk of pupils coming across unsuitable material when they are using the Internet at school:

- We use the local authority approved Internet provider and there is a tight filtering system in place to restrict access to inappropriate materials
- We have a comprehensive Internet Use policy for all pupils and school staff which all pupils and staff sign when they join the school
- A copy of the school Internet Use policy is available on request from the office. It is also available on our school website

Attached to this letter is a copy of the staff and children's agreement forms which form part of the appendices to the policy.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet, as sometimes security can be breached by outside agencies. The school will not be liable for any damages arising from your child's use of the Internet facilities.

We understand that you may want to know more about how your child uses the Internet at home and you can access a range of resources and information on how to help your child keep safe on the Internet at:

www.childnet.com

www.thinkuknow.co.uk

Should you wish to discuss any aspect of Internet use, please don't hesitate to contact me.

Yours sincerely

Mr Jack Goodens

Last Reviewed: December 2019   Next Review: December 2021

Denmead Junior School
Acceptable Internet Use
Please complete, sign and return to the school office

Pupil Name	Year Group/Class:

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and will ensure that my child will abide by these.
I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.   I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.   I agree that the school is not liable for any damages arising from use of the Internet facilities

Signed	Date
Please Print Name	