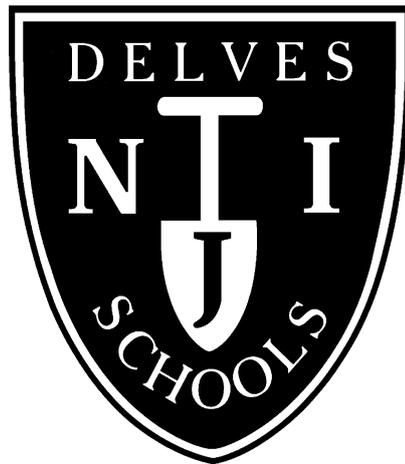# Delves Junior School

Computing/Online Safety

Acceptable Use Policy

Spring 2017

Policy written by: Mr W Howell-Smith
Approved by the Governing Body: _____
Date to be reviewed: Autumn 2017
School/Setting Designated Child Protection Coordinator: Mrs D Manby
School/Setting e-Safety Coordinator: Mr W Howell-Smith
Governor with lead responsibility: Mrs D Reece

Introduction

This policy document sets out the schools aims, principles and strategies for the delivery of the computing curriculum and keeping children safe in this technological age.

The subject is an important curriculum requirement because the ability to use computers effectively is a vital skill in modern society. The policy takes into account equipment that allows the user to communicate or handle information electronically.

Within our school this includes the use of computers, handheld devices, programmable toys, calculators and multimedia resources. This document relates to current practice and plans for further development.

General Aims

Our aims are that
- we meet the requirements of the National Curriculum as fully as possible
- we help all children to achieve high standards at KS2
- we nurture social skills through collaborative group work.
- children can engage in the computing curriculum independently and tackle applications with confidence and a sense of achievement
- children develop practical skills in the computing curriculum and the ability to apply these skills to solving relevant and worthwhile problems across the whole curriculum
- children understand the capabilities and limitations of using computers and implications and consequences of their use

The Schools Approach to the computing curriculum

The school has bought into the Switched On Computing scheme. This scheme has been adapted for use by class teachers throughout KS2 to integrate with the creative curriculum topics. Class teachers deliver computing with the assistance of K Allan (ICT Technician) on a weekly basis. There is currently only one exception to this where W Howell-Smith (Computing coordinator) team teaches the curriculum in Classes 1 and 2 to provide CPD and extra improvement.

Roles and Responsibilities

The roles and responsibilities with regard to Computing are as follows:

Headteacher:

- Ensures staff have access to hardware
- Purchases resources
- Policy central monitoring (staff)

Computing Co-ordinator:

- Oversees continuity between year groups
- Informs Head Teacher and Governors on progress in Computing

All Staff:

- Review the computing policy
- Assess pupils' progress
- Report faults to the ICT technician
- Report to Head Teacher, Computing Co-ordinator and parents on children's progress, share knowledge and ideas

ICT Technician:

- Oversees equipment maintenance
- Organises and purchases resources
- Provides support during Computing lessons
- Acceptable use policy
- Policy central monitoring (children)

Online Safety Co-ordinator:

- Maintains the Online Safety policy
- Ensures children, staff and parents are up to date with Online Safety
- Liaise with Safeguarding lead

Governors:

- Oversee pupil progress
- Oversee budget issues
- Monitor school policy and compliance
- Monitor e-safety

Parents:

- Report any concerns or issues to school
- Informed about their children's progress

Resources

Deployment of hardware is determined through discussion with all the staff.

Year 3	3 interactive whiteboards with 3 desk based laptops, Laptop cabinet with 15 mini laptops
Year 4	3 interactive whiteboards with 3 desk based laptops, Laptop cabinet with 15 mini laptops
Year 5	3 interactive whiteboards with 3 desk based laptops, Laptop cabinet with 30 mini laptops
Year 6	3 interactive whiteboards with 3 desk based laptops, Laptop cabinet with 30 mini laptops
Library	1 interactive whiteboard with a desk based laptop.
Hall	1 pull down projector screen
Lodge	1 promethean touch panel with desk laptop
SMT+Computing	8 mini IPad each
SEN	6 mini Ipad for support
Office	4 desktop computers (admin)

The serial numbers of all computers and iPads are held on the school inventory.
Teachers should notify the technician of all software purchased to be installed on school equipment to ensure relevant network licences are in place.
All staff are aware of data protection issues (appendix)
Every classroom has wireless internet access.

All hardware/software faults should be reported to the ICT technician.

Recording, Assessment and Reporting
Teachers will
- monitor the use of the computers to ensure that all pupils have equal access
- track progress by using the self-evaluations and foundation subject assessment sheet
- keep evidence half-termly evidence of pupils work in the Computing books

Equal Opportunities
Staff recognise that all children should have access to equipment. We will ensure this by checking:

- children in KS2 have equal weekly access for using computers
- that when working in groups or pairs, all children have hands – on experience of the computer
- software and documentation reflect gender and ethnicity in a balanced way
- the teacher responsible for SEND and the Computing co-ordinator jointly advise teachers on the computer support which should be given to children with particular educational needs, this will include children who are gifted and talented

Health and Safety
We consider the safety and comfort of pupils and staff using computer equipment by ensuring:
- Access to websites is filtered. No child is allowed to use the Internet without adult supervision. All pupils and parents must agree to the school's Acceptable Use Policy (Appendix).
- Equipment is easily accessible.
- Staff seating is adjustable
- Users take frequent short breaks from computer work
- There is enough space around a workstation for paper, books and any other materials, including special educational needs equipment
- Staff follow health and safety guidance regarding the height, position and distance of monitors and keyboards from pupils when working
- There is space for more than one pupil at a time, and for the teacher to gain access
- Gangways and emergency exits are kept clear
- When working with programmable toys create a clearly defined working area to ensure that pupils do not accidentally fall over equipment
- That procedures for connecting peripherals (scanners, digital cameras, webcams, control technology/equipment and monitoring equipment), adhere to school and LA health and safety guidelines
- Ensure that pupils do not take drinks to tables if they are working with electrical equipment
- In accordance with the Electricity at Work Regulations Act 1989, all electrical equipment is maintained regularly
- There are the appropriate fire extinguishers positioned in key areas providing full school coverage
- Care is taken to ensure that there are no trailing cables
- Children and staff are educated about the importance of Online Safety

Staff INSET

INSET will be provided where staff identify needs and/or implement new initiatives. Training may take the form of courses offsite or the co-ordinator will conduct in house training or support specific to year group requirements.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Online Safety depends on effective practice at a number of levels:

- Responsible computer use by all staff and students.
- Responsible mobile phone use by all staff and adults in school.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from LA ICT Services including the effective management of filtering.
- National Education Network standards and specifications.

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

Internet use will enhance learning

- The school internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

- Information system security, school computer systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed, revised and updated where necessary with our system managers LA ICT.

E-mail

- Staff and pupils may only use approved (not personal) e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they hear or see anything online.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised in line with current security procedures before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social networking and personal publishing

- The school will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Parents are advised that they should not post information about school, staff or children on social networking sites.
- No staff members will accept parents or children as 'friends' in any social networking site. No comments relating to school, staff or children will be posted to any social networking site.

Managing filtering

- The school will work with LA IT Services LTD, DFE and the Internet Service Provider and Policy Central to ensure systems to protect pupils are continually reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the named Technician
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

- Mobile phones will be switched off at all times while children are in the building. Staff may take devices into safe areas e.g. staffroom or any school office, at break-times to switch on and make or receive personal calls. Consideration will be made if any member of staff has any emergency or safeguarding need on a case-by case basis, and steps will be taken to achieve a safe compromise for all.
- Internal/external staff with mobile devices essential to their role must ensure that they are silenced and if used ensure it is out of sight of the children.
- No member of the school community will be allowed to take photographs of children on their personal phones or other mobile devices.
- The sending of abusive or inappropriate text messages is forbidden.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (see Data Protection Policy)

Computer access

- All staff and Governors will be given the School e-Safety Policy and its importance explained
- All staff must read and sign the 'Acceptable Use Agreement' before using any school computer resources
- Pupils' access to the Internet will be under adult supervision at all times
- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user
- All pupils will be made aware of the school's e-safety rules
- Staff and pupils will be informed that network and Internet use will be monitored
- Parents' attention will be drawn to the School Online Procedures in newsletters, the school brochure and on the school Web site
- Parents will be asked to sign and return an internet access consent form
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Education Walsall can accept liability for the material accessed, or any consequences of Internet access
- Complaints of internet misuse will be dealt with by the Head Teacher and reported to LA ICT
- Online Safety coordinator will undertake an e-Safety audit each year to assess whether the e-safety basics are in place

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not be named, be aware that children at risk will not have photographs published to protect their anonymity.
- Pupils' full names will not be used anywhere on the school website particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and Learning Platform
- Pupil's work can only be published with the permission of the pupil and parents

In addition:

- The ICT Technician is responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the setting/school. This includes the management, implementation, monitoring and review of the School/Settings Image Use Policy.
- Written consent from parents will be kept by the setting where children's images are used for publicity purposes (such as brochures or publications), until the image is no longer in use.
- Parental permission will be sought on an agreed basis on admission to the school.
- Social worker permission will be sought for all images in the case of children who are Looked After or whose family circumstances make this imperative.
- A record of all consent details will be kept securely on file. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of and the record will be updated accordingly.
- Images will not be kept for longer than is to be considered necessary.
- All images will remain on site at all times, unless prior explicit consent has been given by both. Should permission be given to take images off site data will be kept securely (e.g. with appropriate encryption).
- The ICT Technician and/or DCPC reserve the right to view any images taken and/or to withdraw or modify a member of staffs' authorisation to take or make images at any time.
- Any memory stick, CD or storage device containing images of children to be taken offsite for further work will be suitably encrypted and monitored to ensure it is returned within the expected time scale.
- Images or videos that include children will be selected carefully when used online and will not provide material that could be reused.
- Children's' full names will not be used on the website in association with photographs or work.
- The school/setting will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.
- The school/setting will only use images of children who are suitably dressed.
- Children's work will only be published with their permission or their parents consent.
- Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.

- All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.
- Any apps, websites or third party companies used to share, host or access children's images will be risk assessed prior to use. The school will ensure that images are held in accordance with the Data Protection Act and suitable child protection requirements (if necessary) are in place.
- Careful consideration is given before involving very young or vulnerable children when taking photos or recordings who may be unable to question why or how activities are taking place.
- The school/setting will discuss the use of images with children and young people in an age appropriate way.
- Images will not be taken of any child or young person against their wishes. A child or young person's right not to be photographed is to be respected.
- Photography is not permitted in sensitive areas such as changing rooms, toilets, etc.
- Photographs will be disposed of should they no longer be required. They will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies will not to be taken of any images without relevant authority and consent from the Data Controller and/or DCPC and the parent/carer.

All images taken by the school/setting will be used in a manner respectful of the eight Data Protection Principles.

This means that images will be:
- fairly and lawfully processed
- processed for limited, specifically stated purposes only
- used in a way that is adequate, relevant and not excessive
- accurate and up to date
- kept on file for no longer than is necessary
- processed in line with an individual's legal rights
- kept securely

Clarifying School Procedures

- Any images of children captured must be taken on a school device.
- If you or the pupils use a school camera then images should be transferred directly to the school network within 1 week and deleted from the camera. All cameras should have the memory returned before returning to storage.
- If you or the children use a school iPad to capture images these must be transferred to one of the above locations within one week and images must be removed from the internal memory of these devices.
- As an iPad is an encrypted device, staff may take these home for assessment purposes whilst following the above procedures.

Use of Photos/Videos by Parents/Carers

- Parents/carers are permitted to take photographs or video footage of events for private use only.
- Parents/carers are only permitted to take or make recording within designated areas of the setting. Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.
- The opportunity for parents/carers to take photographs and make videos can be reserved by the school/setting on health and safety grounds.
- Parents and carers who are using photographic equipment must be mindful of others when making and taking images.
- The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.
- Parents may contact the school to discuss any concerns regarding the use of images.
- The setting will discuss and agree age appropriate acceptable use rules with children regarding the appropriate use of cameras, such as places children can not take the camera (e.g. unsupervised areas, toilets etc).
- All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official or curriculum use.
- Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos.
- Photos taken by children for official use will only be taken with parental consent and will be processed in accordance with the Data Protection Act 1998.

- Parents/carers will be made aware that children will be taking photos/videos of other children and will be informed how these images will be managed by the setting e.g. will be for internal use by the setting only (not shared online or via any website or social media tool).
- Photos taken by children for official use will be carefully controlled by the setting and will be checked carefully before sharing online or via digital screens.
- Still and video cameras provided for use by children and the images themselves will not be removed from the
- setting.

Use of Images of Children by the Media

- Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's (or other relevant media) requirements can be met. Agreement will be sought between parents and carers and the press which will request that a pre-agreed and accepted amount of personal information (e.g. first names only) can be published along with images and videos.
- The identity of any press representative will be verified and access will only be permitted where the event is planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.
- Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the school is to be considered to have acted in good faith.

Use of Professional Photographers

- Professional photographers who are engaged to record any events will be prepared to work according to the terms of the settings Online safety policy.
- Photographers will not have unsupervised access to children and young people.
- Recordings will be retained for a limited time period only and for no longer than their intended purpose.
- Regular auditing of any stored images will be undertaken by the ICT technician or other member of staff as designated by the management team.

The governors will ensure that:

- Learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- Learners are made aware of risks and processes for safe digital use
- All adults and learners have received the appropriate acceptable use policies and any required training
- The school has appointed an Online Safety Coordinator and a named governor takes responsibility for Online Safety
- An Online Safety Policy has been written by the school, building on the LSCB e-Safety Policy and BECTA guidance
- The Online Policy and its implementation will be reviewed annually
- The school internet access is designed for educational use and will include appropriate filtering and monitoring
- Copyright law is not breached
- Learners are taught to evaluate digital materials appropriately
- Parents are aware of the acceptable use policy
- Parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- The school will take all reasonable precautions to ensure that users access only appropriate material
- The school will audit use of technology (using the Self-Review Framework) to establish if the Online Safety policy is adequate and appropriately implemented
- Methods to identify, assess and minimise risks will be reviewed annually
- Complaints of internet misuse will be dealt with by a senior member of staff

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, network resources, website, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes.

- I will not reveal my password(s) to anyone.

- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

- I will not allow unauthorised individuals to access email/Internet/intranet/network, or other school systems, *or any Local Authority (LA) system I have access to*.

- I will ensure all documents, data etc., are printed, saved, accessed and deleted/shredded in accordance with the school's protecting information procedures.

- I will not engage in any online activity that may compromise my professional responsibilities.

- I will only use the approved email system(s) for any school business.
  This is currently: www.office365.com

- I will only use the approved email system and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- I will not browse, download or send material that is considered offensive or of an extremist nature.

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to a member of the Safeguarding Team.

- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

- I will follow the school's policy on use of mobile phones/devices at school and *will not take into classrooms/only use in staff areas*.

- I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.

- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.

- I will ensure, where used, I know how to use any social networking sites/tools securely, so as not to compromise my professional role.

- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school's protecting information procedures for transporting hard copies of data.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will alert the Designated Safeguarding Lead or a member of the Safeguarding Team if I feel the behaviour of any child may be a cause for concern.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead or a member of the Safeguarding Team.

- I understand that all Internet and network traffic/usage can be logged and this information will be made available to the Head/Designated Safeguarding Lead.

- I will only use any LA system I have access to in accordance with their policies.

- *Staff that have a teaching role only:* I will embed the school's on-line safety/digital literacy/PREVENT agenda into my teaching.

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: ....Date: ....

Full Name: .... (printed)

Job title/Role: ....

Authorised Signature (Interim Head Teacher)

I approve this user to be set-up on the school systems relevant to their role

Signature: .... Date:...

Full Name: Mrs A Arnold

E-safety agreement form: parents

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter/son* access to:

- o the Internet at school
- o the school's chosen email system
- o ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
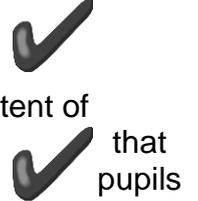
I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

I will help my child understand their Acceptable Use Agreement and ensure it is signed and returned to the school.

My daughter/son name(s): _____

Parent/guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint$^{©}$ presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM/DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- o **Common courtesy**
- o **Common decency**
- o **Common sense**

How do we show common courtesy online?
- o We ask someone's permission before uploading photographs, videos or any other information about them online.
- o We do not write or upload hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?
- o We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- o When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?
- o We think before we click.
- o We think before we upload comments, photographs and videos.
- o We think before we download or forward any materials.
- o We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- o We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.

- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*