Maidwell Primary School

Draughton Road
Maidwell
Northamptonshire
NN6 9JF

Online Safety Policy

History	Details
December 2013	New Policy
November 2014	3.6: Inclusion of school mobile for residential visits 4.3: Inclusion of social network disclaimer message 4.4: School's use of Blogging and Facebook deleted 4.6: Inclusion of eSafety Officer's responsibility to recommend external training if appropriate
March 2016	Policy renamed (was e*Safety Policy*) All references *to eSafety* have been changed to *Online Safety* 1 Kevin Hayle deleted as IT support technician 4.4: School's use of Blogging reinserted in line with Y5 scheme of work
June 2017	Re-ratified. No change made.
January 2018	All references to *Online Safety Officer* changed to *Online Safety Lead* All references to *Safeguarding Sub-Committee* changed to *Online Safety Governor* 2.1: Governor requirement to provide support to Online Safety Lead included 2.1: Online safety to be included as Standing Agenda item 2.1: Online Safety Lead responsible for providing regular updates 3.1: *Illegal Websites* renamed *Blocked Websites* 3.6: Bullet 4 now includes *and a school mobile is not available* 4.4: *Facebook for publicity purposes* now included under Social Networking 4.6: Training programme now *regular* not *annual* 5: *Record of training* deleted and subsequent paragraphs renumbered 11: Checklist updated to include *Administrator password storage, frequency of Online Safety lessons* and *Acceptable Use Policy reissued within last 12 months*
November 2018	2.3: Contact name highlighted for ease of reference 2.8: Reference to Safeguarding Sub-Committee amended
November 2019	Section 5: New section inserted: *Mobile Technology* Subsequent sections (6-12) renumbered accordingly
November 2020	Section 10: New section inserted: *Online Safety Curriculum* Subsequent sections renumbered

The Chair of Governors, on behalf of the Governing Body of Maidwell Primary School, has formally adopted this policy. The Headteacher and the Governing Body will review it no later than one year from the date of signature below.

Last Review	November 2020	Next Review	November 2021
GB Approval Date		Signature Chair of Governors	

Maidwell Primary School

Online Safety Policy

Contents

(Adapted from a model policy provided by ESafety-Advisor.com)

1 Policy Statement

For clarity, this Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, children and any other person working in or on behalf of the school, including contractors who make use of any aspect of IT equipment or IT infrastructure.

Parents – any adult with a legal responsibility for a child outside the school, eg: parent, guardian, carer.

School – any school business or activity conducted on or off the school site, eg: visits, conferences, school trips and residentials etc.

Wider school community – students, all staff, Governing Body, parents, PTA and outside providers (who may only use IT on an infrequent basis).

IT support technician(s) – any member of staff from a technical support company who may visit site. Currently the school uses services from Ashby Computer Services (Andy Hickman).

CEOP: Child Exploitation Online Protection centre – for reporting of inappropriate behaviour online for other persons.

IWF: Internet Watch Foundation – for reporting of inappropriate websites.

Safeguarding is a serious matter. At Maidwell Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as *Online Safety*, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

The primary purpose of this policy is:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to the children or liability to the school

This policy is available for anybody to read on the Maidwell Primary School website; upon review all members of staff will sign the Staff Acceptable Use Policy (AUP).

A copy of the children's Acceptable Use Policy (AUP) will be sent home with children at the beginning of each school year with a parent letter.

This policy works in conjunction with the:

- Behaviour Policy (for children who have not followed the AUP rules)
- Child Protection & Safeguarding Policy
- Anti-Bullying Policy (for dealing with incidents of cyber-bullying)

2 Roles & Responsibilities

2.1 Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents are appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:

    - Liaise with the Online Safety Lead to ensure Online Safety lessons are rigorous and delivered throughout the school on a regular basis
    - Keep up to date with emerging risks and threats through technology use
    - Receive regular updates from the Headteacher and Online Safety Lead in regards to training, identified risks and any incidents
    - Ensure Online Safety is included on the agenda as a standing item at regular Governors' meetings
    - Provide support to the Online Safety Lead when an Online Safety incident has occurred and the school's response needs further consideration
    - Challenge the Online Safety Lead to ensure the school has suitable:

Function:	Firewall	Anti-virus	Internet Filtering	Accredited ISP	Wireless Security
Currently at MPS:	DrayCom Router	ESET NOD	SurfProtect	Exa Networks	WPA-PSK

2.2 Headteacher

Reporting to the Governing Body the Headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Lead, as indicated below.

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up-to-date and appropriate to the recipient, ie: children, all staff, Governing Body and parents
- The designated Online Safety Lead has had appropriate CPD in order to undertake the day-to-day duties
- All Online Safety incidents are dealt with promptly and appropriately.

2.3 Online Safety Lead

The day-to-day duty of Online Safety Lead is devolved to ***Geoff Woods***.

The Online Safety Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use
- Review this policy regularly and bring any matters to the attention of the Headteacher
- Advise the Headteacher and Governing Body on all Online Safety matters
- Engage with parents and the school community on Online Safety matters at school and/or at home
- Liaise with the Local Authority, IT technical support and other agencies as required
- Retain responsibility for supporting staff when they are reporting an Online Safety incident
- Ensure any technical Online Safety measures in school (eg: Internet filtering software, behaviour management software) are fit for purpose through liaison with the Local Authority and/or IT Technical Support.
- Make him/herself aware of any reporting function with technical Online Safety measures, ie: internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing
- Risk assesses new equipment, software and online services to make recommendations to the Headteacher and Online Safety Governor.

2.4 IT Technical Support Staff

(Note: this policy must be brought to the attention of any external technical support agencies and signed by any staff who attend site as if they are a member of staff)

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure and this includes at a minimum:

- Anti-virus fit-for-purpose, up to date and applied to all capable devices
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate
- Any Online Safety technical solutions such as Internet filtering are operating correctly
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are agreed with the Online Safety Lead and Headteacher
- Passwords are applied correctly to all users regardless of age
- The IT System Administrator password is to be used only by technical staff and the IT co-ordinator. (A copy of this password is sealed in an envelope and stored in the school safe)

2.5 All Staff

The boundaries of use for IT equipment and services in this school are given in the staff Acceptable Use Policy.

Staff must ensure that:

- All details within this policy and the associated AUP are understood. If anything is not understood it should be brought to the attention of the Headteacher
- Any Online Safety incident is reported to the Online Safety Lead (and a safeguarding incident report is made) or in his/her absence to the Headteacher. If unsure the matter is to be raised with the Online Safety Lead or the Headteacher to make a decision
- The incident reporting procedures contained within this Online Safety policy are fully understood

2.6 All Children

The boundaries of use of IT equipment and services in this school are given in the children's Acceptable Use Policy; any deviation or misuse of IT equipment or services will be dealt with in accordance with the Behaviour Policy.

Online Safety is embedded into our curriculum; children will be given the appropriate advice and guidance by staff. All children are fully aware how they can report areas of concern whilst at school or outside of school.

2.7 Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' briefings and 1-to-1 support the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will be asked to sign the children's Acceptable Use Policy and discuss the contents of the AUP with their child.

2.8 Online Safety Governor

The Governor responsible for Online Safety will:

- Advise on changes to the Online Safety policy
- Establish the effectiveness (or not) of Online Safety training and awareness in the school
- Recommend further initiatives for Online Safety training and awareness at the school
- Consider risk assessments carried out by the Online Safety Lead

A standing agenda item will be raised at every Governing Body meeting. Where an Online Safety incident or a detailed technical matter is to be discussed the Online Safety Lead is also asked to attend the relevant part of the meeting.

3 Technology

Maidwell Primary School uses a range of devices including PC's, laptops, iPads etc. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

3.1 Internet Filtering

We use Exa Networks SurfProtect software that prevents access to blocked websites. It also prevents access to inappropriate websites as determined by The IT Coordinator/ Online Safety Lead/Headteacher. Changes to the filtering will be agreed by at least two adults from Headteacher, Online Safety Lead, Online Safety Governor and if necessary be referred to the Governors. In this way no single member of staff has the authority/control over changes to the internet filtering.

3.2 Email Filtering

We use ESET NOD software that prevents any infected email attachment to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (ie: malware) that could be damaging or destructive to data; or send spam email such as a phishing message.

3.3 Encryption

All school devices that hold personal data (as defined by the Data Protection Act 1998) are password protected. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are password protected. Any breach (ie: loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Local Authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean just password protected.)*

3.4 Passwords

All staff and students will be unable to access any device without a username and password. Staff and student passwords will change on a regular basis or if there has been a compromise, whichever is sooner. The IT Coordinator and IT Support technicians will be responsible for ensuring that passwords are changed.

Where devices cannot be secured with a password, the IT coordinator, Online Safety Lead and/or technical support technicians will take steps to

secure the devices in another way or ensure they are limited in their functionality to restrict any risk.

3.5 Anti-Virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT support technicians will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

3.6 Mobile phones

- Children are not allowed to use mobile phones in our school.
- Staff are allowed discrete infrequent use of their mobile phone outside of lesson times.
- A personal mobile phone must never be used to record images of children. Only school cameras can be used for this purpose.
- A personal mobile phone must never be used to contact children or parents (unless contact with the parent is an emergency ie: school trip/residential and a school mobile is not available).
- A school mobile will be used while on residential trips to contact parents.

4 Safe Use

4.1 Internet

Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing staff Acceptable Use Policy; to children under strict adult supervision.

4.2 Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted.

Use of a personal email address by staff to contact parents for school purposes is not permitted. Only a school provided email address should be used to contact parents.

Staff are only permitted to contact a child via email if the child has a school email address.

Children are permitted (if deemed necessary) to use the school email system, and as such will be given their own email address. The email address will be made up of a random set of characters so their email account cannot be derived from their name.

4.3 Photos and videos

All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance. Where pictures are released to an outside agency (newspaper etc) children will not be named individually.

A photo/video social network disclaimer will be regularly added to emails and newsletters and displayed at assemblies.

Photographs must only be taken on school cameras/equipment and never on staff personal phones or tablet computers. Cameras/equipment that contain pictures should only be stored in school and not taken home (ie: at the end of a school trip).

4.4 Social Networking

There are many social networking services available. Maidwell Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services have been deemed suitable for use within Maidwell Primary School. Should staff wish to use other social media, permission must first be sought via the Online Safety Lead who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school. A class blog is set up in the Year 5 scheme of work. This will be worked on once every two years. It is used to comment on a class book – all class members post comments and others can comment on these
- Twitter – used by the school as a broadcast service (see below)
- Facebook – used by the school for publicity purposes

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded
- There is to be no identification of students using names
- Where services are "comment enabled", comments are to be set to "moderated"
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (ie: creative commons).

Should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed promptly.

Parents use of social network sites for pictures of children:

It is recognised that parents attending school events may take photos or video. It is highly probable that other children at the event will also be captured on photo/video therefore all parents are asked not to post such images on any social networking site, irrespective of their privacy settings.

A message/poster informing parents as detailed above will be displayed at all such events.

If any postings on social network sites that violate this policy are discovered, the parents responsible for posting the pictures/video will be asked directly to remove them.

Parents' use of social network sites for comments on school and staff:

It is recognised that some parents make extensive use of social network sites to comment on their child's schooling at Maidwell Primary School (facebook, rate-my-teacher…). If any postings on social network sites are defamatory or libellous the parent will be asked, in writing, to directly remove the posting. The school recognises an individual member of staff's right to contact the police and pursue such matters if the parents refuse to comply.

Staff use of social network sites:

It is recognised that some school staff may make use of social networking sites. School IT equipment and the school's internet connection are not to be used for personal access to social network sites.

As a professional person representing the school all staff are expected to:

- not identify any child either by name or indirect reference in a social network posting
- not make defamatory or libellous comments about children, other staff, parents or any other parties linked to the school in a social network posting

Due to the trusted nature of employment in a school all staff need to be aware of situations outside of school where inappropriate pictures may be taken and posted to a social network site.

Staff are encouraged to ensure friends taking and posting pictures that may include themselves ask for their name NOT to be tagged against the picture.

Staff must not 'friend' a child (current or past pupil) on a social network and avoid 'friending' parents where possible.

4.5 Incidents

Any Online Safety incident is to be brought to the immediate attention of the Online Safety Lead, or in his/her absence the Headteacher, and a safeguarding incident report form completed.

In the event of an incident on screen in school, children are taught to switch off the screen and inform an adult WITHOUT closing any windows/applications.

The adult must then:

- Alert the Online Safety Lead/Headteacher immediately
- Ensure the computer is not used further and the monitor stays switched off
- Do not investigate or make an electronic copy (ie: screen capture) to preserve evidence
- Reassure the child
- Complete a school safeguarding incident form

According to the severity of the incident, it may be necessary to contact the Police, CEOP or IWF. These contacts and other actions will be carried out as per the school's safeguarding procedures.

4.6 Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Maidwell Primary School will have a regular programme of training which is suitable to the audience.

Online Safety for children is embedded into the curriculum; whenever IT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the children's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Lead is responsible for recommending a programme of training (including external training where appropriate) and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Children are also taught to recognise how IT can be used inappropriately to carry out bullying, and what to do if they are a victim of cyberbullying.

5 Mobile Technology

5.1 Pupils

Pupils are provided with access to various mobile technology (laptops, iPads, chromebooks) as part of their curriculum.

No child is allocated a 'personal' device or permitted to bring devices from home (BYOD).

The wireless network code is not revealed to any child **in any circumstances**.

Children are not permitted to bring mobile phones to school.

Also refer to Section 7 of this policy for details on children's Acceptable Use Policy (AUP).

5.2 Parents/Carers

Parents/Carers are not permitted to use any personal mobile device in school other than during specific events such as assemblies/performances. During these events, parents/carers are reminded not to use any images outside of their family/personal use (see section 4.3)

5.3 Visitors to the School

Visitors to the school are asked not to use mobile phones in the presence of children.

It is accepted, however, that contractors may need to use mobile technology as part of their reason to visit. However, as all visitors are accompanied whilst in school, they are also monitored in their use of mobile technology.

5.4 Staff

Staff are provided with access to various mobile technology (laptops, iPads, chromebooks).

Staff are not permitted to use any personal devices in the presence of children.

Staff are permitted to connect their personal mobile phone to the guest wireless network for us in the staffroom only.

Also refer to Section 6 of this policy for details on staff Acceptable Use Policy (AUP).

6 Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online Safety policy. Once you have read and understood both you must sign this policy sheet and return a copy to the Headteacher.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the Online Safety Lead and an incident sheet completed.

Social networking – is allowed in school in accordance with the Online Safety policy only. Staff using social networking for personal use (when away from school) should never undermine the school, its staff, parents or children. Staff should not become "friends" with pupils on personal social networks and where possible avoid being "friends" with pupils parents on social networks.

Use of Email – Staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or child, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (ie: staff outings).

Use of Personal ICT - Use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by the Online Safety Lead.

Viruses and other malware - Any virus outbreaks are to be reported to the Online Safety Lead as soon as it is practical to do so, along with the name of the virus (if known) and actions taken.

Online Safety – Like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with children. It is strongly suggested you make use of the online safety resources available at www.thinkuknow.co.uk particularly when planning online safety lessons for your class.

Children's use of ICT – Children must never be left unsupervised when using the internet during a school lesson/activity. Children must not be allowed to use the internet during a wet playtime or wet dinnertime.

Online safety issue identified in school – If you identify an online safety issue in school, or a child has alerted an image/website that is of concern then raise a Safeguarding incident report as per the school's safeguarding procedures. When completing this form ensure the online safety tick box is also completed as this will allow the incident details to be considered from a technical perspective as well as protecting the child.

Name:	
Signature:	
Date:	

7 Acceptable Use Policy – Children

Our Promise of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring.

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anyone inappropriate. If I forget my password I will tell my teacher.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty.

I understand – if I break these rules there will be consequences of my actions and my parents will be told.

I know – to tell an adult I trust if something or someone upsets me on the internet.

We have read these rules together. We have discussed the meaning of these rules and we are confident we understand them. We appreciate the seriousness of using the internet incorrectly in school.

Signed (Child) : _____

Signed (Parent) : _____

Date : _____

8 Letter to Parents

Maidwell Primary School

Draughton Road
Maidwell
Northants
NN6 9JF

Headteacher:
Mrs R James, B.Ed (Hons)

Telephone: (01604) 686240
Fax: (01604) 686240
Email: bursar@maidwell.northants-ecl.gov.uk

Web address: www.maidwellprimary.net

Dear Parents

As part of an enriched curriculum your child will be accessing the Internet and on-line resources via the school's filtered internet connection through use of computers, laptops, tablet computers and other connected hardware.

In order to support the school in educating your child about Online Safety (safe use of the Internet and ICT resources), please read the enclosed rules with your child then sign and return one copy of the rules.

These rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

We would also like to take this opportunity to inform you of our policy regarding photographs and video recording at school events:

You are welcome to use a video or still camera on the understanding any images captured are only for personal or family use.

Any images recorded or stored must NOT be posted to any social networking sites or picture sharing sites.

Images transmitted electronically across the internet (such as via email to other family members) must be sent in a suitably encrypted format.

Yours sincerely

ROSEMARIE JAMES (Mrs)
Headteacher

9 School Posters

Notice to parents before any event where photography/video capture is allowed:

Dear Parents & Friends,

In line with our online safety and child protection policies we would like to make the following statement.

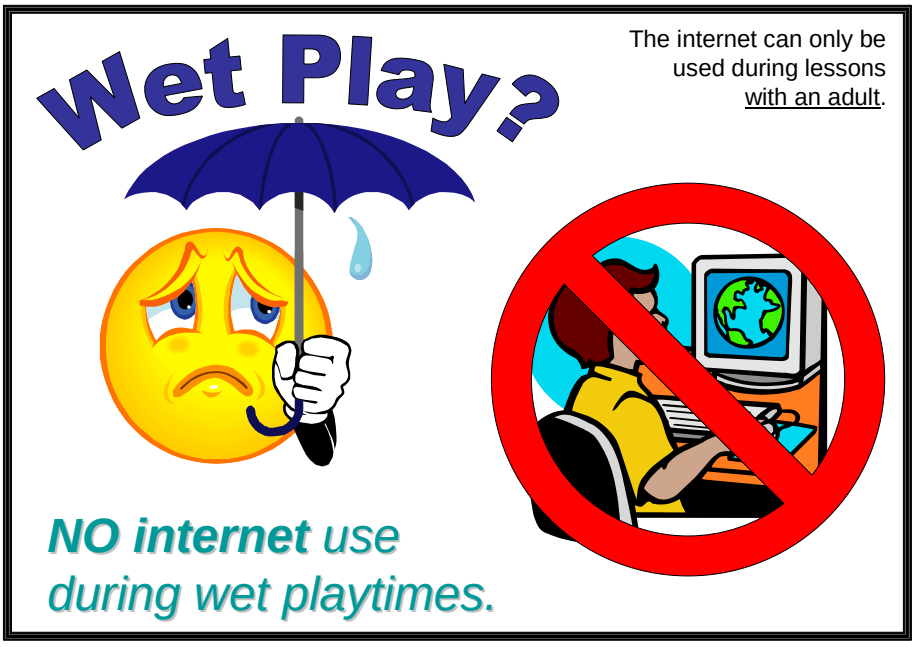
During your time in school you are welcome to use a video or still camera on the understanding any images captured are only for personal or family use.

Any images recorded or stored must NOT be posted to any social networking sites or picture sharing sites.

Images transmitted electronically across the internet (such as via email to other family members) must be sent in a suitably encrypted format.

Thank you.

Notice displayed near computers in classrooms:



Online Safety advice for children – general Online Safety reminders and advice posters are also located around school.

10 Online Safety Curriculum

Online safety is taught within the context of computing lessons and presented as part of the current computing topic being taught at that moment in time.

Three main resources are used to support the teaching of online safety:

- Rising Stars – Switch on eSafety
- Natterhub (https://natterhub.school)
- CEOP / ThinkYouKnow (https://www.thinkuknow.co.uk/)

11 Website links

The following links are provided on the school website or the school internet browser home page:

www.thinkuknow.co.uk
www.kidsmart.org.uk

12 Further Information and Guidance

www.parentscentre.gov.uk (for parents/carers)

www.ceop.co.uk (for parents/carers and adults)

www.iwf.org.uk (for reporting of illegal images or content)

www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)

www.netsmartzkids.org (5 – 17)

www.kidsmart.org.uk – (all under 11)

www.phonebrain.org.uk (for Yr 5 – 8)

www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)

www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)

www.teachernet.gov.uk (for schools and settings)

www.dcsf.gov.uk (for adults)

www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)

(All links above were valid and available at time of inclusion in this policy)

13 Checklist

Online Safety Checklist

This checklist is for the Online Safety Lead and Governor to carry out regular monitoring that all safeguards and procedures are in place, as per the Online Safety policy.

Date checks carried out: _____

Carried out by: _____

	✓ OR Remedial action taken
Network filtering via SurfProtect running correctly	
Anti-virus and anti-spyware software installed on network PCs and in-school laptops	
Staff are aware of the issues regarding internet searching and how to instruct children how to remain safe – in particular with respect to Google	
New Online Safety threats from emerging technologies considered	
Any recent Online Safety incidents considered to ensure technology safeguards have been updated in the light of these events	
New staff have been instructed on data security, anti-virus, filtering and children's Online Safety	
Correct notices / posters are on display in all computer use areas for children and staff	
Administrator password is stored in the safe	
Online Safety lesson(s) have been delivered at least once within the previous term	
Staff and children's Acceptable Use Policy has been refreshed within the previous 12 months	

Further Notes & Action Required: