Learning for Ourselves, Respect, We Can

LYNDHURST INFANT SCHOOL

Online Safety and Acceptable Use Policy

Reviewer: Diane South/Barby Huntingford
Reviewed & Adopted by Full Governors:
Next update: May 2019

Contents:

Aims

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the, ICT manager/co-ordinator and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged in the schools e-safety incident report book and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 5 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing body.

The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics - Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet - Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and social media pages. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet and IT systems in school

Expectations of the ICT User

The following guidelines set Lyndhurst Infant School's expectations for the acceptable use of equipment and use of computers generally around the school by staff and pupils. Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to The Network Manager.

We have created "Acceptable Use Agreement for Pupils" (appendix 1) which, has been designed with the children in mind, for them to understand quickly and easily what is and is not acceptable.

Parents/Carers are asked to sign the Acceptable Use Agreement before their child uses the Internet in school.

Staff are expected to sign the Acceptable Use Agreement upon induction (appendix 2).

Passwords – Passwords are the responsibility of the user and in no circumstances should they be disclosed in any way. If you suspect somebody knows your password then contact the IT System Manager as soon as possible.

Unacceptable Files – On a regular basis the IT Systems Manager will search the network for illegal or unacceptable files; which in turn will be removed.

Network Etiquette and Privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
- Password – do not reveal your password to anyone. If you think someone has learned your password then contact ICT Team.
- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under another user's username should log off the machine whether they intend to use it or not.

Hacking - Hacking into or attempting to corrupt the network settings, software or hardware will not be tolerated. Any attempts to do so will be picked up through regular network checks and will be dealt with by a member of the Senior Leadership Team.

Computer Damage - Any incident of damage to computers (hardware & software) needs to be reported to the IT Systems Manager immediately; this will then be followed up accordingly.

Use of the Internet and e-mail

Lyndhurst Infant School uses a filtered, broadband internet service provider for e-mail and internet access. Pupils and staff will be allowed to use the internet to search for information and resources to meet their professional and learning objectives in school. Pupils and staff will need to be aware that there is no regulatory authority body for the internet, anyone, anywhere can publish materials. It is not censored for opinion, bias or validity of information.

All members of staff must read the West Sussex Guidance for The Safer Use of the Internet by Staff working with Young People a copy of which is held in the school office.

Guidance for school staff regarding social networking sites outside of school

For those who belong to a social networking site (eg Facebook, Twitter, My Space) there are some important issues to note if you want to protect yourself.

- Do not accept any contact with current or previous pupils
- If under 18s are on your list (perhaps family members) be especially careful that the content is appropriate, including photos

- Avoid bad language, sexual connotations, obscene jokes
- Avoid criticism of your employer
- Do not post photos of colleagues without their prior permission
- Check privacy settings and do not post comments that may bring your professional status and the school into disrepute.
- Do not be friends with parents/carers or children you have met through your work at Lyndhurst Infant School

Remember these sites are not always private - often there is a wide access. Ensure that your privacy settings are set to private. Do not say anything that you would not say in public or post comments associated with school which could be easily construed as a breach of confidentiality or even bullying. This is especially important as there have been cases across the country where people have been found to be showing "poor judgment" in relation to professional conduct and/or safeguarding which may be recorded on their permanent record which could affect references.

Use of Digital Images

For the purposes of this section publication includes on websites, including social media, in the press, on TV, as web broadcasts or video/CD/DVD to be released into the public domain.

- Written permission from parents or carers must be submitted to the school before any photo, recording or child's work can be used on the internet including social media sites and local news publicity. (See Appendix 5)
- Named images of pupils must not be published in any circumstance. This includes photographs, videos, TV presentations, web pages, social media, the press etc.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' work can be published (e.g. photographs, videos, TV presentations, web pages, press etc) unless parental objection has been provided in writing.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Photography using mobile phones

The use of a mobile phone to take pictures in school is prohibited. If photos were taken using a mobile phone in school, an allegation could be made that a member of staff has taken inappropriate images with those cameras. Staff are most strongly advised to not use the camera within their personally owned mobile phones whilst on school business. Staff should always use school owned cameras and adhere to the schools policy on photography which outlines where parental permission is required. If a personal phone is used inadvertently, any images must be uploaded to the school network at the earliest opportunity and deleted from the phone with no copies having been kept or transmitted elsewhere and the use reported to the SLT.

Pupils using mobile devices in school

Pupils may not bring mobile devices into school.

Staff using work devices outside school

All staff with access to a school device for use outside of school will be asked to sign a consent form (appendix 4).

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online in the schools e-safety incident report book

This policy will be reviewed annually by the DSL/IT Manager. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Lyndhurst Infant School

Acceptable Use Agreement for Pupils and Parent/Carers

Child's Name:	**Class:**

For the Pupil:

- I will not use the internet or computers unless I have been given permission.
- I will only use activities and/or access websites that I have been told I can use.
- I will tell a teacher or suitable adult if I see any pop ups and I will not click on them.
- I will tell a teacher or suitable adult if I see anything I am not happy with.
- I will not search for offensive material.
- I will only use my username and password and I will not share this with anyone other than my teacher/parent/carer.
- Pupils must only use their class e-mail account. Messages sent must be polite and sensible.
- Pupils are not allowed to bring in removable media such as DVD's USB's mobile devices etc.
- I will take care of the computers and all other equipment.
- I know that if I break the rules I will not be allowed to use the computers/tablets or other IT equipment including the internet.

For the Parent Carer:

- As the Parent/Carer of the child named above, I give permission for my child to use the Internet and E-Mail at school.
- I will make sure that my child understands the acceptable use agreement detailed above.
- I understand that the children will be taught what is acceptable while using the Internet and what is not according to their age.
- I also understand that although the school will take reasonable steps to ensure that my child is supervised, I will not hold the school or County responsible for inappropriate material which my child might obtain, despite supervision.
- I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information.
- I agree to report any misuse of the network to the school.

Signed: Parent/Guardian	Date:
Print Name:	

Appendix 2

Lyndhurst Infant School

Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3

Lyndhurst Infant School

Parental Consent for School Photo, Recording and Work

Child's Name:	**Class:**

Occasionally, we may take photographs and recording of the children at our school. We use these images as part of our school displays and sometimes in other printed publications. We will also use them on our school website, Facebook page and Twitter account.

If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption. If we name a pupil in the text, we will not use a photograph of that child to accompany the article. If a child has won an award and the parent would like the name of their child to accompany their picture we will obtain permission from the parent before using the image.

Learning Journeys and Records of Achievement are used to celebrate your child's progress throughout school. Photographs of individuals, groups or classes of children may appear in these records.

From time to time, our school may be visited by the media who will take photographs or film footage of a high profile event. Children may appear in these images, which will sometimes be published in local or national newspapers, or on approved websites.

To comply with the General Data Protection Act 2018, we need your permission before we can use photographs or any recordings of your child. Please answer the questions below, then sign and date the form where shown and return it to the school office.

Please circle your answer

Q1	I give my permission for my child's work, if selected, to be published on the Internet, including the school website, Facebook and Twitter pages and WSCC websites.	YES	NO
Q2	I give my permission for my child's photograph to be used in Learning Journey/Records of Achievements belonging to other children.	YES	NO
Q3	I give my permission for my child's photograph to be used in publications including the school website, Facebook/Twitter pages and media e.g. local/national newspapers.	YES	NO
Q4	I give my permission for my child to have their school photograph taken, individually and in classes for purchase by parents/carers either digitally or printed and for recordings to be taken i.e. Christmas plays which will be available for purchase by parents/carers.	YES	NO

You have the right to opt out or withdraw consent in respect of one or all of these options at any time. Should you wish to withdraw your consent you will need to notify the school office in writing, or complete a new form and we will update our records accordingly. Opting out will be effective from that date only and will not be retrospective.

Signed: Parent/Guardian Please confirm you have parental/legal responsibility YES/NO	Date:
Print Name:	

Appendix 4

Lyndhurst Infant School

School Device Loan Agreement

Part of Lyndhurst Infant School's Improvement Plan is to provide a mobile device such as laptops/netbooks/iPads/learnpads and or tablets to some staff to assist in the delivery of the Curriculum. The Headteacher has agreed that either device will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time

As a member of staff to whom a device has been loaned I have read and agree to the following terms and conditions that apply while the device is in my possession:

1. The device, and any accessories provided with it, remains the property of Lyndhurst Infant School and is strictly for my sole use in assisting in the delivery of the Curriculum.

2. I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the device is stolen from an unattended vehicle or a house left unattended for longer than 48 hours, I will be responsible for its replacement.

3. I agree to: treat the device with due care and keep the device in good condition, ensure that it is strapped in to the carry case when transported and/or not in use, not leave the device unattended in class without being secured and avoid food and drink near the keyboard/touch pad.

4. I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the device malfunctioning.

5. I agree to only use software licensed by the school, authorised by the Headteacher and installed by the school's IT Manager.

6. I agree that Anti-Virus software is installed and must be updated on a regular basis by bringing the device into school once a month for the IT Manager to update.

7. Should any faults occur, I agree to notify the school's IT Manager as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than the IT Systems Manager, attempt to fix suspected hardware, or any other faults.

8. I agree not to store personal music, pictures or any other media files on this device.

9. I agree that home Internet access is permitted at the discretion of the headteacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.

10. I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.

Device Details

Device…… Make …… Model. ……

Serial Number …… School Code ……

Personnel Details

Loan Authorised by ……

IT Manager: …… Date ……

(signature)

I have read and agree to be bound by the terms and conditions set out above.

Name of Member of Staff ……

Note on Insurance

For a device to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the laptops for theft (where there are signs of forced entry), and accidental or malicious damage. Those Schools who have opted for the additional Buildings and Contents policy will also receive cover for flood/water damage, storm damage etc. All equipment in Schools is automatically covered for fire, lightning and explosion.

Laptops/Netbooks/iPads/Tablets are not covered by the school policy:

- Whilst in vehicles,
- Left unattended in a locked household over 48 hours.

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to ICT staff. If stolen or damaged from an employee's home, County would first ask for a claim under the staff member's household policy. Claims from the School policy will only be made if this were unsuccessful.

Please note that regardless of the policy a stolen device is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

For General Insurance enquiries and claims contact the Insurance & Risk Management team on 01243 777909.

Appendix 5

Lyndhurst Infant School

Online Safety Training Needs Audit

Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	YES/NO
Do you know what you must do if a pupil approaches you with a concern or issue?	YES/NO
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	YES/NO
Are you familiar with the school's acceptable use agreement for pupils and parents?	YES/NO
Do you regularly change your password for accessing the school's ICT systems?	YES/NO
Are you familiar with the school's approach to tackling cyber-bullying?	YES/NO
Are there any areas of online safety in which you would like training/further training? Please record them here.	