LARKHOLME PRIMARY SCHOOL

Online Safety Policy

Mission Statement

- We will create a happy, secure and stimulating learning environment in which all children can grow in confidence, develop their full potential and where academic excellence can be achieved.

- We will provide a nurturing environment and value and recognise the uniqueness of every child.

- We will equip the children with the resilience and perseverance to become creative and independent thinkers and to become learners for life.

- We will provide engaging and varied learning activities across the full breadth of the National Curriculum and equip the children with a thorough understanding of the basic skills of English, Mathematics, Science and Computing.

- We will challenge the children’s minds and bodies and give them a desire to learn and achieve.

- We will promote British Values and ensure the children become caring, tolerant and respectful citizens within the school and wider communities.

- We will prepare children well for the next steps in their lives by promoting self-discipline and the positive mindset which will allow them to aim high in all they do.

- We will ensure children know how to keep themselves safe when using technology.

RESPECT- RESILIENCE- RESPONSIBILITY

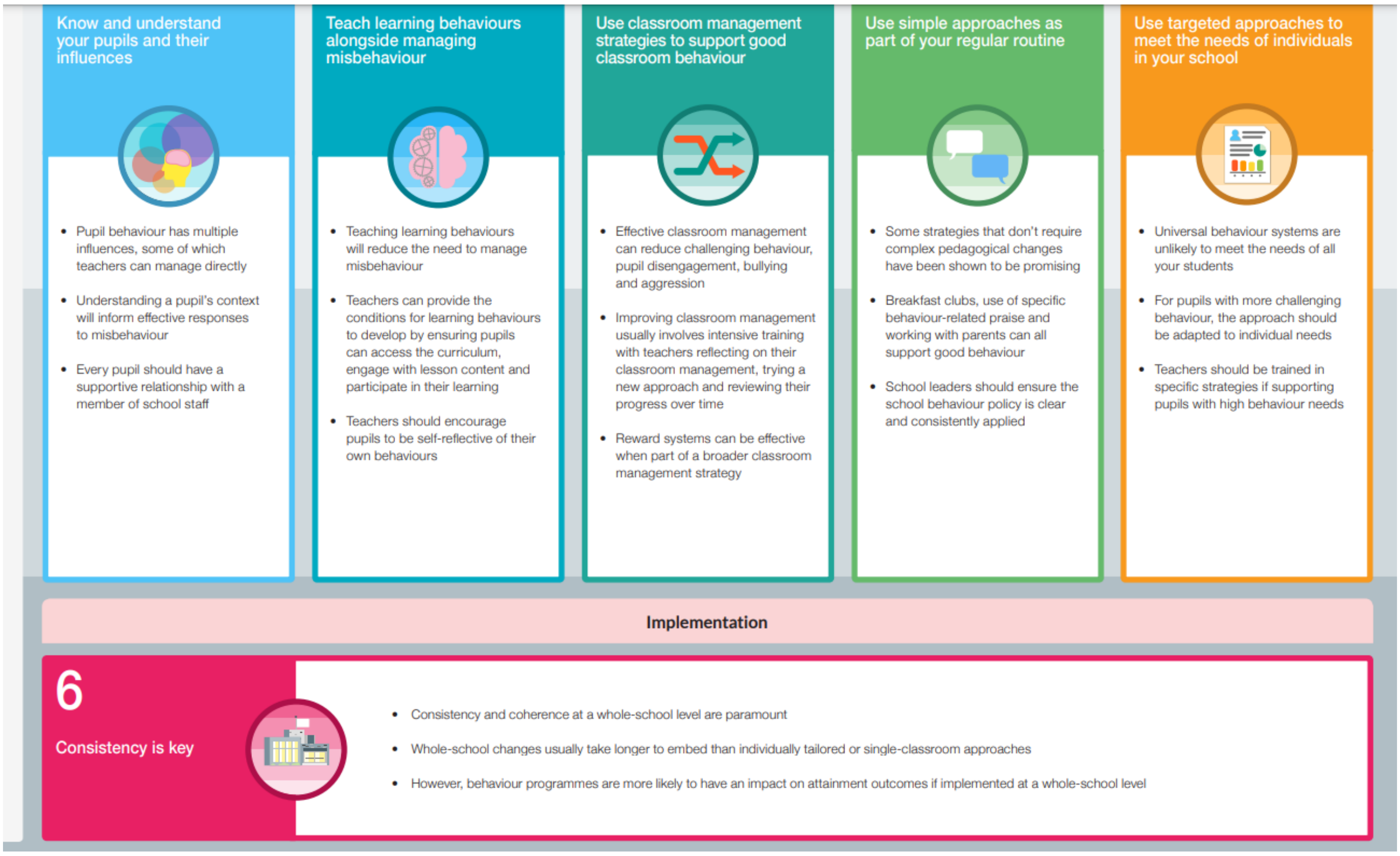
Our Values:

At Larkholme Primary School, we have 3 core values that underpin everything we do.
The 3 core values are:

- Respect
- Responsibility
- Resilience

Alongside our core values, we also promote the fundamental British Values of democracy, the rule of law, individual liberty, mutual respect and tolerance of those with different faiths and beliefs.

Research:



Know and understand your pupils and their influences

- Pupil behaviour has multiple influences, some of which teachers can manage directly
- Understanding a pupil's context will inform effective responses to misbehaviour
- Every pupil should have a supportive relationship with a member of school staff

Teach learning behaviours alongside managing misbehaviour

- Teaching learning behaviours will reduce the need to manage misbehaviour
- Teachers can provide the conditions for learning behaviours to develop by ensuring pupils can access the curriculum, engage with lesson content and participate in their learning
- Teachers should encourage pupils to be self-reflective of their own behaviours

Use classroom management strategies to support good classroom behaviour

- Effective classroom management can reduce challenging behaviour, pupil disengagement, bullying and aggression
- Improving classroom management usually involves intensive training with teachers reflecting on their classroom management, trying a new approach and reviewing their progress over time
- Reward systems can be effective when part of a broader classroom management strategy

Use simple approaches as part of your regular routine

- Some strategies that don't require complex pedagogical changes have been shown to be promising
- Breakfast clubs, use of specific behaviour-related praise and working with parents can all support good behaviour
- School leaders should ensure the school behaviour policy is clear and consistently applied

Use targeted approaches to meet the needs of individuals in your school

- Universal behaviour systems are unlikely to meet the needs of all your students
- For pupils with more challenging behaviour, the approach should be adapted to individual needs
- Teachers should be trained in specific strategies if supporting pupils with high behaviour needs

Implementation

6

Consistency is key

- Consistency and coherence at a whole-school level are paramount
- Whole-school changes usually take longer to embed than individually tailored or single-classroom approaches
- However, behaviour programmes are more likely to have an impact on attainment outcomes if implemented at a whole-school level

Our Rules:

- Ready
- Safe
- Respectful

Adapted from ‘Primary Online Safety Framework Document’, Lancashire Schools' ICT Centre, 2010/2013

Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

- Head Teacher
- Senior Leadership Team
- ICT school technician
- School Governor
- Parents

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Updated - Date: 01.09.2025

The implementation of this policy will be monitored by the Head teacher, R Sims and the ICT school technician.

This policy will be reviewed every 12 months.

Approved by ……………………………………… (Headteacher) Date …………

Approved by ……………………………………… (Governor) Date …………

Contents

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

2. Our school's vision for Online Safety

Our school provides a diverse, balanced and relevant approach to the use of technology. The children are encouraged to maximise the benefits and opportunities that technology has to offer. Our school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively. The children are equipped with the skills and knowledge to use technology appropriately and responsibly. Our school teaches how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. Users in the school community understand why there is a need for an Online Safety Policy.

3. The role of the school's Online Safety Champion

Our Online Safety Champion are R Sims and B Carnell

The role of the Online Safety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring the Online Safety Incident Log (CPOMs) is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by

national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head teacher/ SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

This Online Safety policy should be read in conjunction with the following other related policies and documents:

- Child Protection Policy
- Staff Code of Conduct Policy

4.1 Security and data management

In line with the requirements of the GDPR sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection

All data in our school is kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Staff Acceptable Use Policy.

In order to keep our information secure:

- The school maps key information that is held
- The Headteacher is responsible for managing information
- Relevant staff know the location of data
- Staff with access to personal data understand their legal responsibilities
- The school ensures that data is appropriately managed, both within and outside the school environment, through the use of secure and encrypted emails (as appropriate)
- Staff are aware that they should only use approved means to access, store and dispose of confidential data
- Personal devices, e.g. smartphone, may not be used to access data on the school system

- Risk of data loss is minimised by having daily back-up of both our curriculum and administration networks

4.2 Use of mobile devices

Only mobile devices purchased and recorded to the school may be used to capture images of children. These images may be saved onto the school server but will be deleted from the device as soon as possible. Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of children for their own records during session times.

Personal Mobiles

See mobile phone policy

Photographs and Filming

See Photographs and Filing Policy

4.3 Use of digital media

Please see Photographs and Filming section 4.2 and the Staff Code of Conduct

4.4 Communication technologies

Email

- All users access the Mail 365 service as the preferred school e-mail system.
- Only official email addresses should be used to contact staff/pupils (pupils must not have email accounts which contain their names, using class accounts [e.g. @larkholme.lancs.sch.uk] in preference which can be monitored carefully by the supervising teacher).
- Users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- Users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- Users are aware that they must not open attachments that they suspect may contain illegal content as they may be inadvertently committing a criminal act.
- Users are aware that all email communications may be monitored at any time in accordance with the Codes of Conduct.
- Users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks

Social networking sites are, by default, blocked through the internet filtering system for direct use in Lancashire schools. The safe use of social networking outside of school will be taught.

Websites and other online publications

(including podcasts, videos, 'Making the News' and blogs)

- Staff or pupil personal contact information will not be published. The contact details given online will be the school office.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Group photographs will be used in preference to than full-face photos of individual children.
- Pupils' full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs- unless permission has been given by parents.
- Written permission from parents or carers will be obtained before photographs of pupils are published.
- Pupil image file names will not refer to the pupil by name.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- The school website and social media will be used to communicate Online Safety messages to parents/carers, to provide guidance on the use of digital media.
- Staff are aware what information it is appropriate to publish and what information is not appropriate to publish on the school's website.
- The school's website may be edited by Larkholme Primary School staff only. Pupils may not edit the website.
- Staff are aware that they may not publish content which is subject to copyright / personal intellectual copyright restrictions.
- Downloadable materials will be in read-only format (e.g. PDF) to prevent content being manipulated and potentially re-distributed without the school's consent.

Others

The school's policy will be adapted / updated in light of emerging new technologies. Any issues or risks associated with these technologies, e.g. Bluetooth and Infrared communication will be assessed.

4.5 Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

- Staff and pupils must sign, and visitors and guests must adhere to, an Acceptable Use Policy before access to technology is allowed. Acceptable Use Policies will be displayed by computers and visitors will be given a visitor login with restricted access.
- A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.

4.6 Dealing with incidents

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Potential illegal content must always be reported to the Internet Watch Foundation (http://www.iwf.org.uk).

Examples of illegal offences are:

1. Accessing child sexual abuse images
2. Accessing non-photographic child sexual abuse images
3. Accessing criminally obscene adult content
4. Incitement to racial hatred

More details regarding these categories can be found on the IWF website;

http://www.iwf.org.uk

Any online activity that raises safeguarding concerns must be reported to the DSL

Inappropriate Use- Incident Procedure and Sanctions

It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Accidental access to inappropriate materials

- Minimise the webpage/turn the monitor off/click the ‘Hector Protector’ button.
- Tell a trusted adult.
- Enter the details in CPOMs and report to LGfL filtering services if necessary.
- Persistent ‘accidental’ offenders may need further disciplinary action. (follow behaviour policy)

Using other people’s logins and passwords maliciously

- Inform SLT or designated Online Safety champion.
- Enter the details in the Incident Log on CPOMs
- Additional awareness rising of Online Safety issues and the AUP with individual child/class. (Follow behaviour policy)

More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.

Consider parent/carer involvement.

Examples of more serious offences include:

- Deliberate searching for inappropriate materials
- Bringing inappropriate electronic files from home
- Using chats and forums in an inappropriate way
- Using others' logins/passwords maliciously

Cyber-bullying

The school acknowledges that cyber-bullying may take place in variety of ways, using a variety of electronic means including; email/messenger, mobile phone calls, instant messaging, using someone else's account or phone, chatrooms, websites (including defamatory blogs), social networking sites, electronic games played online, twitter, identity harvesting (where sites and games collect personal details which may leave a child open to stalking/predatory harm), flaming (online fights with angry and vulgar language), harassment, sending or posting gossip or rumours about someone in order to damage their reputation, impersonation, 'outing' (sharing someone's potentially embarrassing information/image online), manipulation online with intent to exploit, isolation (i.e. intentionally and cruelly excluding someone from an online group), cyberstalking and sexting (sending explicit or suggestive images via any new technology).

Incidents of cyberbullying will be dealt with according to the school's Anti-bullying Policy. In the case of serious incidents, the Online-Safety Incident/Escalation Procedure document may be used as a framework for responding to cyberbullying.

Online-Safety incidents will be recorded on CPOMs and findings will be analysed by SLT as part of on-going safeguarding processes.

5. Infrastructure and technology

Filtering / virus protection

- Our Filtering provider (Surf Protect) ensures that access to illegal content is blocked, specifically that the filtering providers: are IWF members, and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

- The school also has devolved filtering which is subject to control measures, a request form will be sent to the technician who will liaise with SLT who have responsibility for unblocking a specific website.
- Sophos Anti-Virus software is included in the school's subscription, is installed on computers in school and configured to receive regular updates.
- Recognising that no filter can guarantee to be 100% effective, our filtering system manages the following content:

Content	Explanatory notes – Content that:
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	displays sexual acts or explicit images
Piracy and copyright theft	includes illegal provision of copyrighted material
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)
Violence	Displays or promotes the use of physical force intended to hurt or kill

- Our filtering system meets the following principles:

Principle
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content
● Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking

● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
● Identification - the filtering system should have the ability to identify users
● Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)
● Multiple language support – the ability for the system to manage relevant languages
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)
● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school
● Reporting mechanism – the ability to report inappropriate content for access or blocking
● Reports – the system offers clear historical information on the websites visited by your users

Pupil access

- Pupils will be supervised when using the internet.
- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network.

Passwords

- Staff have access to a secure username and password which enables them to access their securely stored data and 'staff' section of the server.
- Staff are have signed the staff AUP
- The administrator password for the school network is only available to the ICT Technician, Head Teacher and computing Coordinator.
- Staff are reminded to keep passwords secure.
- Passwords will be changed from time to time.
- Staff will be advised to create passwords containing a mixture of letters, numbers and symbols

Software/hardware

- The school has legal ownership of the software installed on its computers.
- A record is held of licences for all software and this is maintained by the school bursar
- The software installed on the school systems is controlled by the SLT team, ICT technician and computing Coordinator.

Managing the network and technical support

- Servers, wireless systems and cabling are as securely located as possible.
- The security of the school network is maintained by the ICT Technician.
- The safety and security of the school network is reviewed annually with reference to the guidance provided by Lancashire Schools ICT Centre.
- Computers are regularly updated with software updates/patches as required.
- Staff, pupils and guests have clearly defined access rights to the school's network e.g. pupils and guests have restricted access rights to the school's network, and there is a separate server and secure logins for the school administration computers.
- Staff and pupils are required to log out of a school system when a computer/digital device is left unattended.
- Only the network administrator (i.e. the ICT Technician) is allowed to download executable files or install software.
- Users should report any suspicion or evidence of a breach of security to the Head Teacher.
- Removable storage devices may be used in school but sensitive data, including images of children, may not be removed from the school building unless it is on an encrypted device.
- Staff are made aware that network monitoring/remote access may take place.
- External technical support providers (e.g. the ICT Technician) are made aware of the school's online-Safety policy.
- The technical support staff are managed overall by the Head teacher, and on a week to week basis by the computing Coordinator.

Filtering and virus protection

- Filtering is provided by Surf Protect filtering service.
- Filtering is managed by the computing Coordinator/ICT Technician.
- Virus protection (Sophos) is provided through the EDIT subscription and regularly updated.
- The ICT Technician is manages the procedures for blocking and unblocking specific websites.
- Staff must report suspected or actual computer virus infection to the ICT Technician.
- School laptops used at home are set to regularly update virus protection software.

6. Education and training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The three main areas of Online Safety risk (as mentioned by OFSTED, 2013) that the school needs to be aware of are:

Conduct

Area of risk:

Pupils will be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.

Examples of risk Privacy issues, including disclosure of personal information, digital footprint and online reputation. Health and well-being- amount of time spent online (internet or gaming) Sexting (sending and receiving of personally intimate images) Copyright (little care or consideration for intellectual property and ownership-such as music or film

Content

Area of risk:

Pupils will be taught that not all content is appropriate or from a reliable source.

Examples of risk:

Exposure to inappropriate content, including:

- Online pornography
- Ignoring age ratings in games (exposure to violence associated with often racist language)
- Substance abuse
- Lifestyle websites, for example, proanorexia/ self-harm/suicide sites, hate sites

Contact

Area of risk:

Pupils will be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.

Examples of risk:

- Grooming
- Cyber-bullying in all forms
- Identify theft (including 'frape'- hacking Facebook profiles)
- Sharing passwords

6.1 Online Safety across the curriculum

Pupils are taught how to take a responsible approach to their own Online Safety. Suitable Online Safety education is provided to all pupils through:

- Regular, planned Online Safety teaching, following the national curriculum (adapted for those with SEN as necessary).

- An additional focus on Online Safety during National Online Safety Awareness Week
- Take part in Safer Internet Day activities

In addition pupils learn:

- About Cyberbullying and how to seek help if affected by these issues (via Kid Safe training).
- To critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- To develop an understanding of the importance of the Acceptable Use Policy and how to use ICT safely and responsibly both within and outside of school.
- About copyright.
- Also, pupils are reminded of safe internet use through display of the Online Safety rules.

6.2 Online Safety – Raising staff awareness

- Regular formal Online Safety training is provided for all staff so that they are regularly updated on their responsibilities as outlined in our school policy.
- Advice/guidance or training for individuals, as and when required, will be provided by the ICT Coordinators or other appropriate individuals.
- Members of staff delivering training will have received external Online Safety training/updates from a county provider/CEOP.
- Online Safety training will ensure that staff are made aware of issues which may affect their own personal safeguarding e.g. the use of social network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school’s Online Safety policy and acceptable use policy.
- Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed in staff/team meetings.
- Staff to be aware of their own digital footprint

6.3 Online Safety – Raising parents/carers awareness

“Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.” (Byron Report, 2008).

Larkholme Primary School offers regular opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies.

For example through: school newsletters, the school's website, bespoke Parents Online Safety Awareness sessions and promotion of external Online Safety resources/online materials.

6.4 Online Safety – Raising Governors' awareness

- Governors, particularly those with specific responsibilities for Online Safety, ICT or Child Protection, are kept up to date through discussion at Governors' meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.
- The Online Safety Policy is regularly reviewed and approved by the governing body.

7. Standards

- The effectiveness of the Online Safety policy will be monitored through planning scrutiny, lesson observations, interviews with staff and pupils, and monitoring of website access, downloading and email accounts as appropriate.
- Online Safety incidents will be monitored and recorded by the Online Safety Champion and the I.C.T. Technician.
- The introduction of new technologies will be risk assessed and these assessments included in the Online Safety policy.
- Any recurring incident will be analysed to see if there is a recurring pattern e.g. e.g. specific days, times, classes, groups and individual children.
- Monitoring of Online Safety incidents will contribute to changes in policy and practice as necessary. Any changes to policy and practice will be reported to staff and governors through meetings, to pupils by their teacher and to parents via the school newsletter / website.
- AUPs will be annually reviewed and include reference to current trends and new technologies.

Related Documents...

Appendix 1 – Example of Image Consent Letter to Parents

Appendix 2 – Example of Acceptable Use Policy (Staff)

Appendix 3 – Example of Acceptable Use Policy (Parents/Children)

Appendix 4 – Example of Typical Online Safety Rules

Appendix 5 - Example of Letter Inviting Parents to Online Safety Awareness Sessions

Appendices

APPENDIX 1 - Example of ICT Acceptable Use Policy (AUP) – Staff and Governors

Larkholme Primary School

Windermere Avenue, Fleetwood, Lancashire, FY7 8QB ☎:01253 874024 email:office@larkholme.lancs.sch.uk

LARKHOLME PRIMARY SCHOOL. ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: 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 (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- 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, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

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 and my use of the school's ICT facilities and systems.
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 2 - ICT Acceptable Use Policy (AUP) for Parents and Children

Larkholme Primary School

Windermere Avenue, Fleetwood, Lancashire, FY7 8QB ☎:01253 874024 email:office@larkholme.lancs.sch.uk

LARKHOLME PRIMARY SCHOOL. ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS.

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

APPENDIX 3 - Example of Typical Classroom Online Safety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

APPENDIX 5 - Example of Typical Classroom Online Safety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.