Edisford Primary School

Confidence. Persistence. Getting Along. Organisation. Resilience.

E-Safety Policy

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; contact: being subjected to harmful online interaction with other users and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Filtering and Monitoring

The school uses the LGfL filtering service known as 'NETSWEEPER'. The effectiveness of this is checked regularly.

We have a clear system of filtering and monitoring:

*weekly sweep of websites accessed across school using Netsweeper carried out by the IT technician.
*IT technician reports any issues to the DSL.
*Computing Lead is informed if there are any e-safety issues to incorporate in the curriculum.
*Class teachers are trained.
*Filtering and monitoring provision is reviewed annually.
*Checks are run regularly so that filtering and monitoring does not unreasonably impact teaching and learning or school administration.

*pupils are taught within the computing curriculum about assessing and managing risks themselves.
*our filtering and monitoring provider is a member of the Internet Watch Foundation (IWF) and is signed up to the Counter Terrorism Internet Referral Unit list.
*blocking access to illegal content, including child sexual abuse material.

We recognise that our filtering and monitoring system cannot be 100% effective. We understand the coverage of NETSWEEPER and its limitations and the IT technician, the Computing lead and the DSL work to minimise harm and to meet the statutory requirements in KCSIE and the PREVENT duty.

Monitoring

Monitoring activity on school devices is an important part of providing a safe environment for children and staff. We monitor user activity regularly, pick up on incidents urgently and take prompt action. We record the outcome.

Forms of monitoring include:

*physical monitoring of staff watching screens of users.
*network monitoring using log files of internet traffic and web access (IT technician).

The governing body check that appropriate filtering and monitoring systems are in place. The governor responsible is Johanna Blackburn.

DSLs, IT technicians and the computing lead undertake training to ensure their knowledge is current.

Prevent Duty

This monitoring and filtering system supports the safeguarding of children by ensuring they cannot access terrorist and extremist material when using the internet and that suitable supervision is in place.

Responsibilities

Headteacher: overall responsibility for leading filtering and monitoring systems in school.

DSL: responsibility for ensuring these systems protect children and keep them safe from harm online.

Prevent lead: responsibility for ensuring these systems protect children from access to terrorist and extremist material when using the internet.

Computing lead: responsibility for working with the filtering and monitoring team to set up systems and monitor online safety.

IT Technician: to support all of the above with the technical aspects of the filtering and monitoring system.

The SLT will take responsibility for:

- procuring filtering and monitoring systems;
- documenting decisions on what is blocked or allowed and why;
- reviewing the effectiveness and overseeing reports;
- training staff to follow policies and act on reports or concerns.

Virus Protection

We use Sophos Intercept X to protect our school systems for viruses. We check the effectiveness of this regularly and any breaches are recorded and virus threats removed.

Through our Computing Curriculum and PSHE, we teach our children these golden rules:

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.

We don't give out personal information on any online forums.

Vision for E-Safety

We provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer.

We ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively. We acknowledge that children need access to content which will inform and educate. We carefully review sites that are useful for this in order to avoid 'over blocking'. Children are equipped with the skills and knowledge to use technology appropriately and responsibly.

We teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.
All users in our school community understand why there is a need for an e-Safety Policy.

Our e-Safety Champion is Elizabeth Hamilton-Thorpe. She has:

- Operational responsibility for ensuring the development, maintenance and review of the school's e-Safety Policy and associated documents, including Acceptable Use Policies.
- She will ensure a Behaviour and e-Safety Incident Log is appropriately maintained and regularly reviewed.
- She will keep personally up-to-date with e-Safety issues and guidance from the document Keeping Children Safe in Education, through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Provide e-Safety advice/training for staff, parents/carers and governors.
- Ensure the staff, children and governors are updated as necessary.

Security and data management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment.

The *Lancashire ICT Security Framework* (published 2005) should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school. In line with the requirements of the General Data Protection Regulation (GDPR, 2018) and the Data Protection Act (2018),

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.
- Staff are aware that they should only use approved means to access, store and dispose of confidential data.
- We do not use cloud storage facilities e.g. Dropbox / OneDrive or external storage related to software used for creation of children's profiles (especially in Early Years).
- Key computers are password protected.
- No devices containing data allowed to be removed from the school premises.
- Staff are not allowed to store data on personal devices.

Cyber Security

Wherever possible, we endeavour not to email personal information with more than two pieces of personal data. All staff have school email accounts using Outlook 365. This is accessed through two-factor secure authentication.

The head and office computer are password-protected with private, secure, strong passwords. These measures work to reduce the risk of a cyber incident.

Use of Mobile Communication Devices

Please refer to our Mobile Communication Devices Policy.

Photographs/Videos of Children - Consent

We have ***written*** consent from parents for photographs and/or videos of their children to be taken or used. Parents are consulted regarding material for: newsletter, website, Instagram and local media.

Verbal consent is not considered acceptable.

A record of non-consent is maintained by the bursar and disseminated to all teaching staff.

Students are not allowed to take photos to include in portfolios maintained by trainees/students not directly employed by the setting.

Taking Photographs / Video

Photographs/videos are only taken using school owned equipment. The use of personal equipment to store images should be avoided.

Storage of Photographs / Video

Storage of such visual images must be stored on password protected computers in school and not in the 'cloud'.

CCTV, Video Conferencing, Zoom and Webcams

During lockdown 2020/21, when the school was only partially open, Zoom video conferencing was used to maintain contact with pupils not in school.

Parents agreed to adhere to a set of terms and conditions for use of Zoom with their children, which included: online etiquette, appropriate backgrounds and content (see Appendix 7).

Managing the network and technical support

Our ICT technician is responsible for managing the security of the school network and for installing all programmes.
This is reviewed annually with safeguarding training.

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, 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.

Inappropriate use

It is more likely that we will need to deal with incidents that involve inappropriate rather than illegal misuse. Any incidents are dealt with quickly and actions are proportionate to the offence. These are logged in our e-Safety Incident Log. Historically, most of these incidents have arisen from inappropriate use outside of school, which school have been made aware of.

Education and training

Children are taught that third-party contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies. As such, they could be at risk from:

- Child-on-child abuse
- Grooming
- Cyberbullying in all forms
- Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.

Conduct

Children are made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others, for example,

- 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) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

E-Safety - Across the Curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' e-Safety.
Our school has brought in a new ICT and Computing scheme which encompasses e-safety, taught throughout every year group in a sequential way. In this way, we aim to prepare children for life in an increasingly technological world.
Updated July 2025.
Review date July 2026.

APPENDIX 1

Example of Image Consent Letter/Form to Parents

Edisford Primary School
Edisford Road, Clitheroe BB7 2LN
Telephone 01200 422239

Dear Parents,

In line with data protection rules in effect in the UK from **25th May, 2018** (GDPR), we would like you to confirm your choices regarding photos and videos of your child.

These, as well as copies of children's work, are invaluable to showcase and celebrate the activities undertaken by pupils in school and we would, therefore, appreciate you taking the time to confirm your consent.

Name of child…… DOB…….

Please tick (✓) ONE of the following options and return this form to school.

1. I consent to the following:

   - Photos and videos of my child, as well as copies of their work, to be used on the school website and in the school newsletter.
   - Photos of my child to be used in their own books (exercise books, Endeavours scrapbooks).
   - Photos of my child to be used in other children's books (exercise books, Endeavours scrapbooks), e.g. group shots.
   - Photos of my child to be shared with local media e.g. newspaper or marketing.
   - Photos and videos of my child being used on the school's social media page (Instagram)

   ☐

***** OR *****

2. I do **NOT** give consent for the school to use **any** of the above. ☐

If you change your mind at any time, please let us know by contacting the school office.

Parent or carer's signature: …… Date: ……..

By signing this agreement, you confirm that you will not publish photos of other children on any public domain. **This means that information cannot be shared or published in any way, e.g. photos cannot be published on social media or displayed in a public place.**

Please note that the Privacy Notice is available on the school website: http://www.edisford.lancs.sch.uk

APPENDIX 2

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

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in e-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms and accessing inappropriate material.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights. We recommend that all staff use Pixabay.com to access royalty free images.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of the Computing lead and SLT.
10. I will notify the Computing Lead and SLT in the event of a security breach or failure of both the NetSweeper filtering system and the Sophos Intercept X virus sweeper system.
11. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
12. I will ensure that images of children and/or adults will be taken, stored on a password protected staff computer and used for professional purposes in line with school policy. School will also gain written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image. Any pictures taken on

our school mobile phone will be uploaded as soon as possible to a password protected staff computer and deleted from the device immediately.

13. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

14. I will report any known misuses of technology, including the unacceptable behaviours of others.

15. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

16. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

17. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

18. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

19. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

20. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's e-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.

21. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name .....(PRINT)

Position/Role .....

APPENDIX 3

Example of ICT Acceptable Use Policy (AUP) –
Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored on a password protected staff computer and used for professional purposes in line with school policy. School will also gain written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image. Any pictures taken on our school mobile phone will be uploaded as soon as possible to a password protected staff computer and deleted from the device immediately.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……

Date ……

Full Name ……(PRINT)

Position/Role ……

APPENDIX 4

ICT Acceptable Use Policy – Children

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.

We don't give out personal information on any online forums.

Child's Name..... (print)

Child's Signature.....

Class .....

Date .....

APPENDIX 5 ICT Acceptable Use Policy (AUP) – Letter to Parents

Dear Parent/Carer,

The use of ICT, including the Internet, e-mail, learning platforms and mobile technologies, are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network sites that incorporate age-restriction policies, where the minimum acceptable age is at least 13 years. Any child who is below the acceptable age and who sets up or uses such a site is in clear breach of the site's privacy policy and/or terms and conditions. We, therefore, actively discourage such practices in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School E-Safety Policy, and alongside the school's Behaviour and Safeguarding Policies, outlines those principles we expect our children to uphold for both their own benefit and that of the wider school community.

Your support in achieving these aims is essential and I would, therefore, ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Our school provider operates a filtering and monitoring system that restricts access to inappropriate materials. This is called NetSweeper. As part of this, we seek to ensure that harmful content is effectively filtered and any breaches are acted upon swiftly through a robust monitoring system.

If you would like to find out more about e-Safety for parents and carers, please visit the Lancashire e-Safety website:
http://www.lancsngfl.ac.uk/esafety

Yours sincerely,
Elizabeth Hamilton-Thorpe

APPENDIX 6. Zoom Parental Agreement

Dear Parents,

Please read the following agreement, which sets out guidelines for use of Zoom with children learning at home.

Parent/Pupil Video Conferencing Agreement

We ask that:

- You access Zoom through parent / guardian accounts and make sure that the name of user is the child's first name only. This is so the hosting teacher can identify who is in the waiting room and will be able to let them into the session. Any names the teacher cannot identify, or have not signed the agreement below, will not be allowed to join the session.

- You, or an appropriate adult, are present in the room during the call and appropriate behaviour and language must be maintained at all times.

- Children are in a suitable environment during the call and that they are appropriately dressed.

- Household members are aware that the call is taking place and background noises and conversations can be picked up.

- You do not share the meeting login details with anyone outside of your household.

- You do not record the session or post or share sound, images or video clips of the teacher or other children that attend the Zoom session.

*****If there is a breach of the above rules, the child will be removed from the session and put into the waiting room or the call will be ended for all users.**

We will:

- Use the waiting room feature on Zoom, which will be administered by the hosting teacher.

- Use secure passwords to keep sessions secure.

- Mute children at times to allow others to speak and to improve sound clarity.

- Not use the live recording facility but may take screen shots to share on social media where we have permission to do so.

Please note: Unlike when we are in school, your child will be using your internet connection, which may not have the controls and firewall settings that we have when we are at school. We encourage you to review your home internet settings.

In participating or allowing your child to participate in online/remote learning, you are acknowledging that you understand that your child's image and voice will be transmitted via the Internet, into the homes of other pupils and staff. You are also acknowledging that the school, while taking measures to ensure secure transmission, cannot guarantee complete confidentiality (see pupil rules above) of your child's image/voice while participating in online learning.

Parents must also understand and agree that recording and/or dissemination of a child's or a staff member's voice and/or image is a serious school rule violation that may subject a child to the loss of online privileges and/or other disciplinary action, as appropriate. This may, in extreme cases result in a report to the appropriate authorities and the potential issuance of criminal charges. The parent and pupil agree that by participating in these online activities, they or any individual present in the pupil's household will not, without express written authorisation from school personnel, audio/video record or transmit other student or staff voices, images, or work product.

Please e-sign this document and return it to bursar@edisford.lancs.sch.uk to agree to the terms set out above.
I agree to the terms of use for Zoom video calls for my child
……

E-signed: _____ (Please type name) Date: _____