Our vision: **‘Let your light shine’** based on Matthew 5.16

Egglescliffe C.E. Primary School

Durham and Newcastle Diocesan Learning Trust

(DNDLT)

Company Number 10847279

E-Safety Policy

Updated: October 2023

Review: October 2024

Contents:

Statement of intent

Egglescliffe C.E. Primary understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

This policy follows the guidance set out in the 'DfE: Teaching Online Safety in Schools 2023' and coincides with the schools Online Safety Policy.

1. Monitoring and Reviewing

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for computing, bullying and for child protection.

- The schools E-Safety Lead will work in collaboration with the Head Teacher (Mrs E. Robertson), the designated safeguarding lead.
- Our e-Safety Policy has been reviewed by the Head Teacher. The e-Safety Policy and its implementation will be reviewed annually or in response to an incident using the attached audit (Appendix 5).

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and other mobile devices).

As the children's access and understanding expands, so should the guidance and rules to ensure safe access use of the internet. Any changes made to this policy are communicated to all members of the school community.

The next scheduled review date for this policy is **October 2024.**

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the E-Safety Lead's remit covers e-safety.
- Ensuring they understand the issues and strategies at our school in relation to local and national guidelines and advice.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The headteacher will be responsible for:

- Ensuring that e-safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Updating the governing board and SLT about any current e-safety issues at our school in relation to local and national guidelines and advice.
- Supporting the E-Safety Lead by ensuring they have enough time and resources to carry out their responsibilities in relation to e-safety.

- Organising engagement with parents to keep them up-to-date with current e-safety issues and how the school is keeping pupils safe.
- Working with the E-Safety Lead and governing board to update this policy on an annual basis.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Monitoring online safety incidents to identify trends and any gaps in the school’s provision, and using this data to update the school’s procedures.

The E-Safety Lead will be responsible for:

- Taking the lead responsibility for e-safety in the school.
- Liaising with relevant members of staff on e-safety matters, e.g. the SENCO and ICT technicians.
- Keeping updated with current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.
- Ensuring e-safety is recognised as part of the school’s safeguarding responsibilities and that a coordinated approach is implemented.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school’s e-safety policies and procedures.
- Implementing appropriate security measures as directed by the Head Teacher.
- Ensuring that the school’s filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of e-safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school’s reporting procedure.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.

- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting e-safety incidents and concerns in line with the procedures within this policy.

3. Importance and benefits of the internet in the school

The internet is an essential element in 21st century life for education and teachers, parents and pupils need to develop good practice in using the internet as a tool for teaching and learning. The school has a duty to ensure internet use is as safe as possible which will enable increased use and the quality of that use is a critical factor.

Internet access provides a service designed for pupils and can stimulate discussion and creativity, whilst increasing awareness of context to promote effective learning. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. This includes the use of a filtering system in school that is appropriate to the age of pupils.

- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the curriculum requirement.
- Pupils will be given clear objectives for internet use.
- Staff will select sites that will support the learning outcomes and are age suitable. .
- Pupils will be educated in taking responsibility when accessing the internet.

Several studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils world-wide.
- Access to experts in many educational fields
- Staff professional development - access to educational materials and good curriculum practice.
- Communication with peers and professional associations
- Improved access to technical support.
- Exchange of curriculum and administration data with DDMAT the LA and DfE.

The effective and safe use of these innovative and progressive technologies has proven to raise self-esteem and impact directly on pupil progress.

4. Managing Internet Access

Pupils, staff and other members of the school community will only be granted access to the school’s internet network once they have read and signed the Acceptable Use Agreement.

- Internet access will be granted to a whole class as part of the scheme of work, after a suitable education in the responsible use of the internet (e-safety).
- Pupils will agree set rules in each class on the acceptable use of the internet
- Parents will be informed that pupils will be provided with supervised internet access.

- All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

5. Managing Filtering

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The E-Safety Lead, Head Teacher and ICT Technician will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The Head Teacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Blocking strategies will be applied to remove access to a list of unsuitable sites or newsgroups. ICT technicians will maintain the updating of the list of sites blocked and school staff will raise any concerns if they arise. Filtering will be applied to examine the content of web pages, emails and internet searches for unsuitable words, resulting in the blocking of access.

Requests regarding making changes to the filtering system will be directed to the Head Teacher. Prior to making any changes to the filtering system, ICT technicians and the E-Safety Lead will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the E-Safety Lead and ICT technicians, who will resolve the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices, including pupils, will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the E-Safety Lead and Head Teacher who will manage the situation in line with the Safeguarding and Child Protection Policy.

6. Information System Security

The Internet is a connection to the outside world that could compromise system performance or threaten security.

- Security strategies will be discussed with the One IT our service provider.
- The authority is regularly reviewing the schools' networks to ensure that the system has the capacity to take increased traffic caused by Internet use.
- The security of the whole system will be reviewed regarding threats to security from Internet access.
- Personal data should not be sent over the internet from school.
- Virus protection will be installed and updated regularly.
- Personal use of memory sticks on school devices needs specific permission granted, be encrypted, and have a virus check.
- Use of e-mail to send attachments will be monitored closely.
- School ICT systems capacity and security will be reviewed regularly with One IT.
- Staff have access to the server remotely, rather than using memory sticks to store information.
- The Head Teacher, E-Safety Lead and ICT Technicians will ensure that the school adheres to the policies and procedures set out in the Cybersecurity Policy and Information Security Policy.

7. Keeping pupils and parents safe online

The school will ensure that regular communication with pupils and parents is made regarding E-safety and current issues. Advice and information will be provided using expert providers, including NSPCC, National Online Safety, Childnet and others.

- Pupils of all ages will complete a unit of work on E-safety each year.
- Filtering and monitoring systems used to allow safe internet access.
- Pupils will be taught to tell a trusted adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils and staff will use equipment responsibly in line with the Acceptable Use Agreement.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.
- Online Safety workshops will be offered to parents on a yearly basis.

8. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.

- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Regular Online Safety updates via School PING
- Newsletters
- Online resources

9. Publishing Pupil's Images and Work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they always use equipment in a respectful and safe manner in accordance with the Acceptable Use Agreement.
- Published photographs will only include images of children where permission from a parent/carer has been given and will not disclose a pupil's full name.
- Where pupil's work is published the school will ensure that the child's identity is protected.

10. E-Safety in the Curriculum

E-Safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Computing
- Relationships and health education
- PSHE

E-Safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour

- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum and are evident in our scheme of learning for Computing (Kapow).

- Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.
- External visitors may be invited into school to help with the delivery of certain aspects of E-Safety in the curriculum. The Head Teacher and E-Safety Lead will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are taught about the impact of Cyberbullying and how to seek help if they are affected by any form of online bullying.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum**.**
- Regular activities will be organized to make E-Safety a high focus in school such as Safer Internet Week and Cyberbullying Week.
- Computing scheme of work (Kapow) incorporates E-Safety into bespoke lessons and other curriculum areas.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding and Child Protection Policy.

11. E-Safety Skills Development for Staff

The E-Safety Lead and Head Teacher will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff will be kept informed with any updates to the E-Safety curriculum and will complete yearly training on online safety. New staff and student teachers receive information of the school's Acceptable Use Policy as part of their induction and will be required to read sign the Internet and Social Networking Statement (Appendix 1). All staff are aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

12. Complaints Procedure regarding Internet Use

Concerns regarding a pupil or staff member's online behaviour should be reported to the Head Teacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the issue has arisen through internet use inside or outside school. Transgressions of the rules could include minor as well as the potentially serious consequences and a range of sanctions will be devised, linked to the school's Behaviour Policy.

13. Managing Emerging Technologies

Mobile Phones:

- Pupils are not permitted to have mobile phones upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However we discourage this on security grounds as they are easily lost, damaged or stolen. Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the class teacher and locked away safely for the duration of the day. We expect pupils not to carry a mobile phone in school. If they do, then they are handed into the school office (switched off) on a morning and collected at home time.
- Only school cameras are to be used by both staff and children for educational purposes.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.

Social Networks

Facebook, X, Whatsapp, SnapChat and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff *are not* permitted to access their personal social media accounts using school equipment at any time.
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are made aware that the information, comments, images and videos they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are made aware that their online behaviour should at all times be compatible with UK law and have signed the Social Networking Policy within school.

Appendix 1

Egglescliffe CE Primary
<u>Internet and Social Networking Statement</u>

Name of Staff Member :……………………………………..

Date:………………………………………………………….

<u>I have received or been directed to the policies below and I agree to uphold these policies in school:</u>

- Laptop Protocol for Teachers and School Support Staff
  (Laptops from school may only be used for work related activity and not for personal usage.)

- E-Safety Policy (please refer to staff shared area on system to view)

  (We always promote guidance on keeping safe on the internet and recognise our duty to report any misdemeanour)

- Acceptable Internet Usage Statement for All Staff

  (We abide by the security mechanisms provided for the school internet system and digital imaging policy)

- Internet and Social Networking Statement
  (Under no circumstances do we publish photographs or personal information about colleagues or children in school on social networking sites- this includes photographs of school social events and the spreading of confidential inform eg. Results from external monitoring such as Ofsted.)

Signed
…………………………………………Date…………………………………

(please sign and return this form only to your school office)