Duston Eldean Primary School

'TOGETHER WE GROW'

At Duston Eldean, we encourage a **reflective, creative, caring and respectful** environment where the whole school community is **happy, enthused and motivated**.

In developing a **love for learning** we sow the seeds of success.

Online Safety and Acceptable Use Policy

Signed …… Signed ……

(Chair of Governors) (Head teacher)

Date …… Date ……

Date of Adoption: January 2024

Frequency of Review: January 2025

Annual Review Date due:

Online Safety Policy for School Employees 2023/24

1. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. Schools must, through their Online Safety and Acceptable Use Policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e. policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

"24. All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content" (KCSIE, 2023)

2. Scope of policy

This Online Safety and Acceptable Use Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). The Online Safety and Acceptable Use Policy should be used in conjunction with the school's disciplinary procedures and code of conduct applicable to employees and pupils. It:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the delivery of the policy.
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- describes how the school will help prepare learners to be safe and responsible users of online technologies.
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction, online safety training and accessible through the shared network.
- is published on the school website.

3. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within legislative and advisory documents such as:

Working Together to Safeguard Children 2018
Keeping Children Safe in Education 2023
Counter Terrorism and Securities Act 2015
Searching, Screening and Confiscation Advice for schools 2022
Teaching Online Safety in School 2023
Meeting digital and technology standards in schools and colleges 2023

Online safety behaviours are also regarded in other school policies. Copies of these can be found on the school website or requested via the school office. They include:

Behaviour policy
Child Protection and Safeguarding Policy
Anti-bullying Policy
Prevent Policy
Code of Conduct Policy

All safeguarding responsibilities of schools and individuals referred to within this Online Safety and Acceptable Use Policy includes, but is not restricted to the legislation listed above.

4. Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of our school community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders

The headteacher and senior leaders have overall responsibility for online safety as part of the wider remit of safeguarding and child protection. The roles of the headteacher and senior leaders are detailed below:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and (at least) deputy/DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

Governors are responsible for the approval of the Online Safety and Acceptable Use Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the Safeguarding Governors Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Lead.
- regularly receiving (collated and anonymised) reports of online safety incidents.
- checking that provision outlined in the Online Safety and Acceptable Use Policy (e.g. online safety education provision and staff training is taking place as intended).
- reporting to relevant governors and the Safeguarding Committee.
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible).

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

The Online Safety Lead will:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.
- have a leading role in establishing and reviewing the school online safety policies/documents.
- promote an awareness of and commitment to online safety education and supporting the senior leaders to raise awareness across the school and beyond.
- create a suitable, discrete and progressive online safety curriculum and liaise with year group leaders to ensure that the curriculum is embedded and evaluated.
- ensure that online safety education is promoted through assemblies and relevant national initative opportunities e.g. Safer Internet Day and Anti-Bullying Week.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- receive reports of online safety incidents and log incidents (EDUKEY) to inform future online safety developments.
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners.
- liaise with technical staff, pastoral staff and support staff (as relevant).
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs.
- attend relevant governing body meetings/groups.
- report regularly to headteacher/senior leadership team and to meet at least annually to review the filter and monitoring provision (unless in the event of a safeguarding risk identified when this should happen immediately or when new technology is introduced)
- liaise with the local authority team online safety lead.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers

- potential or actual incidents of grooming
- online bullying.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety and Acceptable Use Policy and practices.
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use agreement (AUP) (See Appendix 1)
- they immediately report any suspected misuse or problem to *Stacey Ramm and Cathy Moore* for investigation/action, in line with the school safeguarding procedures.
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- they ensure learners understand and follow the school ONLINE safety acronym during their use of school technologies.
- they teach the Online Safety Curriculum as stated to ensure children receive a breadth of understanding about how to navigate themselves online.
- they supervise and monitor screens during use of digital technologies (including laptops, ipads and kindles) and implement current policies regarding these devices.
- in lessons where internet use is pre-planned, learners should be guided to sites checked as suitable for their use.
- processes are in place for dealing with any unsuitable material that is found in internet searches.
- where lessons take place using live-streaming or video-conferencing, this should be discussed in advance with the Online Safety Lead so appropriate checks and guidance can be given.
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- risk assessments for trips and residentials should include use of technology for communication purposes.

Network manager/technical staff

At Duston Eldean Primary School, we employ the technical services of Easipc Services Ltd (EasiPC Services Ltd – Outstanding ICT Support for Schools & Academies). The Easipc technical staff are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy.
- the school technical infrastructure is updated with the required security and firmware updates following the ISO 27,001, Cyber Essentials Plus standards and the meeting digital and technology standards in schools and colleges policy.
- there is clear, safe, and managed control of user access to networks and devices.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Stacey Ramm and Cathy Moore for investigation and action.

- To ensure the filtering system recommended and implemented is a member of Internet Watch Foundation (IWF), is signed up to Counter-Terrorism Internet Referral Unit List (CTIRU) and blocks access to illegal content (to include CSAM- Child Sexual Abuse Material). The filtering system should also have the capacity to identify technologies and techniques that allow users to get around the filtering such as VPNS and Proxy services and block them.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Learners
They:

- are responsible for using the school digital technology systems in accordance with the school learner acceptable use agreement and Online Safety and Acceptable Use Policy **(See Appendix 3).**
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety and Acceptable Use Policy covers their actions out of school.
- are able to understand the school's ONLINE acronym to help reinforce best practice to stay safe online.

Parents and carers
Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety and Acceptable Use Policy, the school ONLINE acronym and a copy of the learners' acceptable use agreement on the school website.
- publishing information about appropriate use of social media and online behaviours.
- seeking their permissions concerning digital images.
- information evenings, newsletters, our website and social media messages with information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in reinforcing the online safety messages provided to learners in school.

Volunteers
We welcome volunteers to support children with their learning in school and to support on visits. Volunteers are asked to complete an agreement which includes a statement on the use of technology. (See Appendix 4)

Acceptable Use Code of Conduct
The Online Safety and Acceptable Use Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction;
- splash screens on school devices;
- posters/notices around where technology is used;
- communication with parents/carers;

- online safety sessions;
- the school website.

All school-based employees, including volunteers, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- ensure that any school IT equipment used for pupil use is booked out through the calendar system linked to Outlook. This is to ensure that a log of use is kept to help with monitoring.
- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner (see appendix 3).
- report any online incident, concern or misuse of technology to the Online Safety lead, Headteacher or DSL, including the unacceptable behaviour of other members of the school community.
- only use school ICT systems and resources for all school related business and communications involving sensitive pupil data or information.
- If authorised by a member of the extended leadership team (ELT), personal technology such as mobile phones and i-pads may be used to take photographs/videos/audio recordings of children engaged in school related activities only. The purpose of the image/video/recording should be to support children's learning or for sharing through official communication channels (i.e. school Facebook account, Twitter, Parentmail, Itslearning, Tapestry). These images must only be taken on a personal device if authorised by a member of ELT. Once shared for the intended purpose, the digital artefact must be correctly and permanently deleted from the device (See appendix 8- permission form for using personal technology)
- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile/phone numbers, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.
- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- not invite, accept or engage in communications with children from the school community (past or present) on any personal social networking sites.
- protect their passwords/personal logins and log-off the network wherever possible when leaving devices unattended.
- understand that network activity and online communications **on school equipmen**t (both within and outside of the school environment) will be monitored. This includes when using school equipment on any other wifi network.
- understand that activity on the school network using any personal device will be monitored.
- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

- When investigating claims of child-on-child online abuse, a child's mobile device (if onsite) can be requested to be looked at to ascertain correct information to help with the investigation. In this situation, the child and another member of staff should be present when looking at the device. Where possible, ask the child to show you only the information that you are looking for. If the device is not onsite, notify parents/carers to guide them to the information that is needed, or request they bring in the device to help in dealing with the situation.

- If a member of staff suspects an indecent image of a child (sometimes known as nude or semi-nude images) is on a device, they should immediately inform a DSL. Staff, including DSLs, **should never** intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response.

- Understand that if you have knowledge of any adult working within school who fail to comply with the professional obligations listed above, procedures stipulated with the Whistleblowing policy should be followed.

The Acceptable Use of Technology Agreement should be signed on appointment by all staff members. (See Appendix 1). When joining the school, parents/carers will be given a copy of an Acceptable Use Agreement seeking permission for their children to access the internet. (See Appendix 2)
Children are taught rules to ensure their safety when online. This should be taught and referred to during weekly reflection time and discreet online safety lessons (See Appendix 3)

5. Online Safety Curriculum (Appendix 9)
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (Appendix 8)

- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learners' needs and progress are addressed through effective planning and assessment.
- Incorporating/making use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.

6. Filtering and Monitoring
Through working with our filtering provider and IT technician, the school ensures that the infrastructure/network is as safe and secure as is reasonably possible.

Filtering- Provided by Securly

- the school filtering policies are agreed in discussion with senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- access to online content and services is managed for all users.
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated and reports are regularly ran and reviewed.
- there are established and effective routes for users to report inappropriate content.
- any changes made to the filtering settings should be requested through either the Online Safety Lead, DSL or DSL deputy. **This should not be requested directly through the Easipc portal or IT technician. Any changes to be logged by the online safety lead, DSL or deputy DSL (Appendix 10)**
- Filtering logs are sent weekly to online safety lead, DSL and deputy DSL and are regularly reviewed. These alert the school to breaches of the filtering policy, which are then acted upon.
- In the event that a personal mobile device has been allowed internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- ensuring internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the Online Lead, DSL and Deputy DSL of breaches to the filtering policy, allowing effective intervention.
- staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be via email to either DSLs or Online Lead, with clear reasons for the need.

7. Inappropriate Use by staff

Examples of inappropriate use include:

- accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

- sharing of pupils' personal information/pictures through non-agreed channels i.e. social media with members of staff, parents or others.

- behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

In the event of staff misuse

If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher immediately. If the allegation is against the Headteacher, the Chair of Governors should be contacted. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- EPM (Human Resources)
- Designated Officer (Formerly known as LADO- Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the Online Safety Incident Flowchart (Appendix 5) and procedures following misuse by staff. (Appendix 5)

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed if appropriate.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

In the event of inappropriate use by a child or young person

In the event of access to inappropriate materials, students are expected to notify an adult immediately.

Please refer to Procedures following Misuse by Children/Young People (Appendix 7)

8. Policy Review

The Online Safety and Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable use rules for students should be consulted upon

annually with the school community to ensure that all young people can understand and adhere to expectations for online behaviour.

9. Useful Links

https://www.nasuwt.org.uk/advice/health-safety/social-media-the-abuse-of-technology/protecting-yourhttps://www.nasuwt.org.uk/advice/health-safety/social-media-the-abuse-of-technology/protecting-your-privacy-online.htmlprivacy-online.html NASUWT Social Networking- Guidelines for Members)

https://neu.org.uk/advice/online-safety-protecting-school-staff-and-pupils
(NUT E-Safety: Protecting School Staff- Guidance for Members)

https://www.ceop.police.uk/safety-centre/
(reporting system for children, parents and professionals)

www.thinkuknow.co.uk
(information and resources for children, teenagers, parents/carers and professionals)

https://www.childnet.com/resources (resources for professionals and parents)

https://www.net-aware.org.uk/ (social media guide for professionals and parents)

https://nationalonlinesafety.com/guides (app guide for professionals and parents)

https://www.commonsensemedia.org/ (app guide for professionals and parents)

T:\2. Curriculum Resources\Esafety Curriculum (Online safety curriculum resources on staff share)

Appendix 1 - Staff Acceptable Use of Technologies Agreement

To ensure that all staff are confident in their use of technologies and the internet, the Acceptable Use Rules have been developed in collaboration with education professionals and unions. The core values of the Acceptable Use Policy are safeguarding and responsible behaviours allowing young people, and the adults who surround them, to safely enjoy all of the benefits that technology can offer. To assist with this, the full Acceptable Use Policy is accessible to all staff members and should be referred to for further information.

The Online-Safety Lead is: Stacey Ramm (ICT/Computing Lead))

The Designated Safeguarding Leads for Child Protection are:

Cathy Moore (Head Teacher and DSL)
Andy Stevenson (Deputy Head Teacher)
Catherine Smyth (Assistant Head Teacher)
Emma Bateman (Family Support Worker)
Jane Other (Safeguarding Governor)
Chris Pettitt (Online Safety Governor)

- I know that I should only use the school equipment in an appropriate manner and for professional use.
- I understand that to support appropriate monitoring of ICT use, I must ensure that any school equipment being used by pupils is booked out via the calendar system linked to my school email address.
- I understand that I must not have personal communications with current, or former pupils, outside of my professional role. This includes establishing social networking 'friendships' on sites such as Facebook, or sharing personal phone numbers or email addresses. Any school-related communication should be conducted through professional email accounts or telephone numbers only.
- I understand that I should not behave in a manner, either within or outside of the work environment, which would lead any reasonable person to question my suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on myself, my colleagues or the school.
- I know that permission must be received from parents/carers before images of children are used online (e.g. school website). I understand that images must be appropriate and should not reveal any personal information, including first names given on social media sites.
- In the event that a personal device is used to take photographs or videos, the digital artefact created must be authorised by a member of ELT and permanently disposed of as soon as possible.
- I understand that any incidents of concern for children's safety must be reported to the Headteacher, Designated Safeguarding Leads for Child Protection and Online Safety Lead in accordance with procedures listed in the Online Safety Policy
- I know where to access a copy of the Online Safety Incident Flowchart should an incident of misuse arise.
- I understand that the school email system and school issued devices will be monitored as part of the school's commitment to safeguard young users.

- I understand that my online activity will be monitored whilst using the school wifi (on school or personal devices) and whilst using a school device on any wifi network, including home.

- I know that any proposed changes I would like to make to the filtering settings should be requested through either the Online Safety Lead, DSL or DSL deputy. This should not be requested directly through the Easipc portal or IT technician.

- I know that each user should be accessing the internet with their class unique username and password for filtering and safeguarding purposes. For this reason, I will keep my password private and for my own use only.

- I will raise any concerns regarding school ICT use with the Online Lead to avoid possible misunderstandings.

- I have access to a copy of the full Online Safety and Acceptable Use Policy should I need to refer to the document about any online-safety issues or procedures.

- I will immediately report any damage or faults involving equipment or software, however this may have happened. If I am unable to access the reporting system (Easipc Portal), I will notify my ELT lead to report on my behalf. - https://portal.easipc.support/

- I will seek parental/carer permission when I have need to look on a child's device when investigating an online safety incident. Where an incident refers to a suspicion of an indecent image, I shall not look at the image and notify the DSL/DSL Deputy.

- I understand that if I have knowledge of any adult working within school who fail to comply with the professional obligations listed above, I should follow the procedures stipulated with the Whistleblowing policy.

- I have read, understood and agree to the above Acceptable Use rules. I understand that these rules are in place to ensure that staff are aware of their professional responsibilities to safeguard children when accessing online technologies.

Signed: …….. Dated: ……

Appendix 2 – Parent/Carer Acceptable Use of Technologies Agreement

Accessing the internet
As part of an enriched curriculum, your child will be accessing the internet, school email and virtual learning environment via a filtered service provided by Securly. In order to support the school in educating students about safe use of the internet, we are asking parents and children to read and sign acceptance of the attached acceptable use rules. Completed forms should be returned to the school as soon as possible.

The rules provide an opportunity for further discussions with your child about safe and appropriate use of the internet and other online tools (e.g. mobile phones), both within and beyond school (e.g. at a friend's house or at home).

Further Information and Guidance

- https://www.ceop.police.uk/safety-centre/ (reporting system)
- www.thinkuknow.co.uk
- https://www.childnet.com/resources
- https://www.net-aware.org.uk/ (social media guide for professional and parents)
- https://nationalonlinesafety.com/guides (app guide for professionals and parents)

Social Media
Digital technologies have become an important part of our lives. These technologies provide powerful tools which open up new opportunities for everyone. As such, we have established a Twitter and Facebook account for the school. Through the use of social media, we hope to help parents facilitate discussions with their children about the school day, celebrate the teaching and learning within the school and model best practice in how to navigate social media safely and effectively.

Our social media is not intended to replace face to face discussions with members of staff and any worries or concerns should be communicated in person, by telephone or by email.

Please note, in order to safely manage these accounts and protect anonymity:

- You will be unable to post anything to the wall (only comment on what the school has posted)
- You will be unable to private message the school through Facebook or Twitter
- You will be unable to 'tag' us into any of your personal posts.
- We will use class names but will not name any individual children.

We intend to post pictures of children in school at work and also outside on school trips. Please indicate on the form below whether or not you give consent for your child to have photographs on our school website, Facebook and Twitter accounts.

If you would like to discuss any reservations before giving permission, please speak to Miss Stacey Ramm, our Online Safety Lead (Year 2 Otters).

Please note, we expect only adults to follow/like any posts submitted on social media. The table below lists current social media platforms and their minimum age restrictions.

Social Media Platform	Minimum Age	Social Media Platform	Minimum Age
Facebook	13+	Twitch	13+
Instagram	13+	X (Twitter)	13+
Kik	13+	Viber	13+
Tiktok	13+	Whatsapp	16+
Roblox	7+	Youtube	13+
Snapchat	13+		

Devices within school

Children from Year 5 onwards are permitted to bring in a mobile device to school. Children should only bring in these devices if they are walking to and from school without an adult. If children are not walking to school, we would expect these devices to stay at home. In some individual cases, some children from Year 4 can bring a device if they walk home without an adult, and the same rules will apply.

When devices are bought into school, they will be switched off once they are on school grounds. Devices are handed into class teachers, who lock them away in a secure place. These are then retrieved at the end of the day, where they are not to be switched on until off school grounds.

In the event of a reported online safety issue and the device is in school, the school will contact you to obtain your permission to check your child's device with your child with another member of staff present.

Wearable Technology

As a school, we encourage children to be aware of their health and their physical activity. We allow children to wear devices that help count their steps throughout the day. Digital watches are also permitted, but all associated alarms should be turned off during the school day.

We do not allow devices which are internet enabled or communicative in anyway. This includes smart watches.

We look forward to sharing our school day with you.

Many thanks

Miss Stacey Ramm and Mrs Cathy Moore

Permission slip re: Accessing the internet and Social Media

Childs Name:

Class:

Accessing online - Parent/Carer Agreement:

- I have read and discussed the rules with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the internet, email and other online tools.
- I understand that filtering can never be completely fool proof and occasionally inappropriate materials may be accessed. I accept that the school will endeavour to deal with any incident that may arise swiftly and according to policy.
- I understand that my child's safe use of the internet and online technologies outside of school is my responsibility.

Social Media- please tick where appropriate

□ I give permission for my child's photograph to be used on the school website and social media accounts, throughout their time at Duston Eldean Primary School.

□ I do not give permission for my child's photograph to be used on the school website and social media accounts, throughout their time at Duston Eldean Primary School.

Devices in school (Yr5 + Yr6 parents/carers only)

- I understand that mobile devices should only be sent into school if my child is walking to and from school without an adult.
- I understand that any device bought into school is switched off and locked away during the school day.
- I understand that any wearable technology that is internet enabled or can be used as a communicative device should not be bought into school.

Parent/Carer Signature: _____ Date: _____

Appendix 3 - Child Acceptable Use of Technologies Agreement

I will listen and follow the advice from my online safety lessons

I will listen and follow the rules set by my teacher when I am using devices in school and my trusted adults at home

I will think and reflect on my online behaviour during our reflection time lessons

I will think and follow the school rules of ONLINE to ensure I am staying safe

Obey rules set by trusted adults

Never be rude online

Lies can appear online

Information about you is private

Nasty feelings should be shared with a trusted adult

Everyone has the right to feel safe online

Name: _____**Class:**_____

Child Signature: _____ **Date:** _____

Appendix 4- Volunteer Agreement

Volunteering at Duston Eldean

Thank you for volunteering to help in school- your time and commitment are much appreciated.

Please sign below to acknowledge that you have received and understood information regarding:

- **Safeguarding**
  Any concerns regarding a child's welfare should be reported to a member of staff. Designated Safeguarding Leads are Cathy Moore, Andy Stevenson, Emma Bateman and Catherine Smyth.
- **Technology**
  Please refrain from using mobile phones when working in school. Under no circumstances should photographs or recordings be made of children.
- **Evacuation procedures**
  If the fire alarm rings, exit and meet on the playground netball court. In the event of a lockdown, stay in classrooms, lock doors and hide under tables away from windows.
- **Confidentiality**
  Under no circumstances should information regarding pupils be shared with anyone other than school staff. Any queries should be referred to class teachers.
- **Concerns**
  If you have any concerns regarding health and safety or a person in school (adult or child) please report to the Headteacher. If your concerns are regarding the headteacher, you should report to the Chair of Governors or Deputy Headteacher.

Name……..

Date……

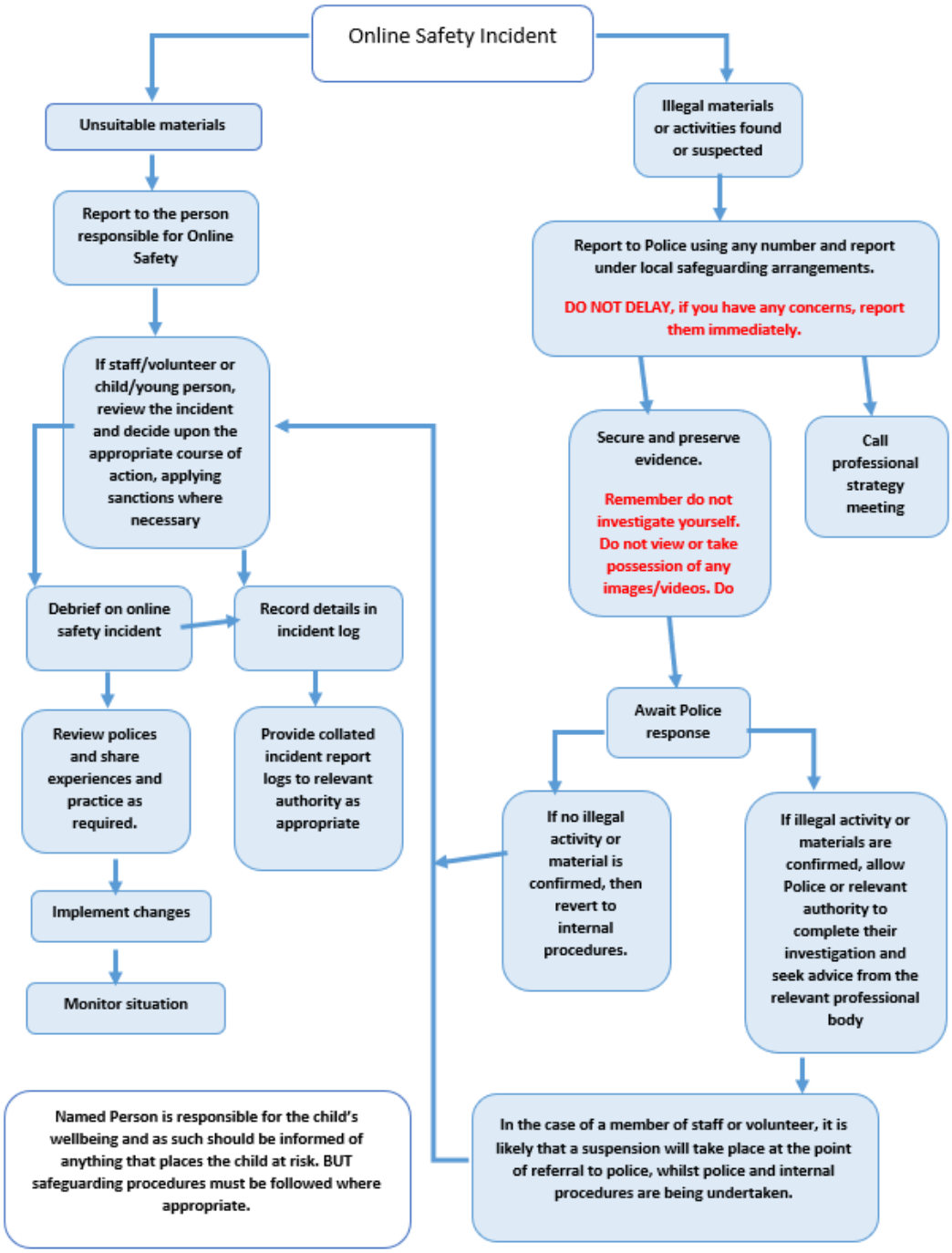
Signature……

Appendix 5 – Online Safety Incident Flowchart

There are three instances when you must report directly to the police.

- Indecent images of children found (i.e. under 18 yrs of a sexual nature)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. The police will advise on how to deal with the machine if they are unable to send out a forensics team immediately. If in doubt, do not turn off the machine. The Internet Watch Foundation www.iwf.org.uk offers further support and advice in dealing with offensive images online. It is important to remember that any offensive images received should never be forwarded, even if it is to report them as illegal, as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.



Appendix 6- Staff Procedures following Misuse by Staff

The Head Teacher will ensure that these procedures are followed. In the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:

Report website to the Online Safety Lead, DSL or DSL Deputy. If this is deemed necessary. they will add this site to the banned list immediately.

B. An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down.
- Log the incident by completing a purple form
- Report website to the Online Safety Lead, DSL or DSL Deputy.
- Head Teacher to refer back to the Acceptable Use Rules and follow disciplinary procedures.

C. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Head Teacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately: Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Head Teacher and Designated Safeguarding Lead for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, Northamptonshire Safeguarding Board.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Head Teacher or Chair of Governors (if allegation is made against the Head Teacher) and Designated Safeguarding Lead for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the Head Teacher immediately and follow Disciplinary Procedures as necessary.
- Inform the Local Authority's Designated Officer and Online Safety Lead so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. Where staff or adults have posted on inappropriate websites, or have inappropriate information about them posted, this should be reported to the Head Teacher.

H. Where any of these incidents apply to the Headteacher, the Chair of Governors will be responsible for its implementation.

Appendix 7- Staff Procedures following Misuse by Children/Young People

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the E-safety lead if this is deemed necessary.
- E-safety lead will add site to the banned list immediately.

B. An inappropriate website is accessed deliberately:

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Head Teacher and Designated Safeguarding Lead for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Head Teacher must follow the Allegation Procedure and/or Child Protection Policy.
- Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website about a child in school:

- Preserve any evidence.
- Inform the Head Teacher immediately.
- Inform the E-safety lead.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Head Teacher immediately.

Appendix 8- Permission Form for Using Personal Technology

Duston Eldean Primary School

'TOGETHER WE GROW'

Permission Form for Using Personal Technology

If authorised by a member of the Extended Leadership Team (ELT), personal technology such as mobile phones and i-pads may be used to take photographs/videos/audio recordings of children engaged in school related activities only.

This form should be completed by a member of the ELT and signed by the identified member of staff.

Date:

Class/children:

Purpose of photographs/videos/audio recordings:

Please read and sign that you understand and will abide by the following:

- Adults should remain sensitive to any pupil who appears uncomfortable and should recognise the potential for misinterpretation. It is also important to take into account the wishes of the child, remembering that some children do not wish to have their photograph taken.
- Ensure that all photographs/images are available for scrutiny, if required, to screen for acceptability
- No images of pupils should be taken for personal use
- Do not take photographs in one to one situations in a private space
- Do not display or distribute photographs/images of pupils unless there is consent to do so from the parent/carer
- Only publish images of pupils where their parent/carer have given explicit written consent to do so
- Do not take images of pupils in a state of undress or semi-undress
- Do not take images of pupils which could be considered as indecent or sexual
- Do not take images of a child's injury
- Do not make audio recordings of a child's disclosure
- Once shared for the intended purpose, the digital artefact must be correctly and permanently deleted from the device.

Member of ELT: Signature:

Member of staff: Signature:

Appendix 9- Online Safety Curriculum

Duston Eldean Primary School

"TOGETHER WE GROW"

Project Evolve- E-safety Curriculum						
Year Group	Term 1- - Online Relationships	Term 2- Online reputation	Term 3- Self- Image and Identity	Term 4- Online Bullying	Term 5- Managing Online information/Privacy and Security/ Copyright and Ownership	Term 6- Health, Well-being and Lifestyle
EYFS	I can give examples of how I (might) use technology to communicate with people I know	I can identify ways that I can put information on the internet.	I can recognise, online or offline, that anyone can say 'no' - 'please stop' - 'I'll tell' - 'I'll ask' to somebody who makes them feel sad, uncomfortable, embarrassed or upset.	I can describe ways that some people can be unkind online.	I can identify devices I could use to access information on the internet.	I can identify rules that help keep us safe and healthy in and beyond the home when using technology
YR1	I can give examples of when I should ask permission to do something online and explain why this is important.	I can describe what information I should not put online without asking a trusted adult first.	If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust and how they can help.	I can describe how to behave online in ways that do not upset others and can give examples.	I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke.	I can explain rules to keep myself safe when using technology both in and beyond the home.
YR2	I can explain why I have a right to say 'no' or 'I will have to ask someone'. I can explain who can help me if I feel under pressure to agree to something I am unsure about or don't want to do.	I can explain how information put online about someone can last for a long time.	I can explain how other people may look and act differently online and offline.	I can explain what bullying is, how people may bully others and how bullying can make someone feel.	I can explain why some information I find online may not be real or true.	I can explain simple guidance for using technology in different environments and settings e.g. accessing online technologies in public places and the home environment.
YR3	I can explain what it means to 'know someone' online and why this might be different from knowing someone offline.	I can give examples of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal.	I can explain ways in which someone might change their identity depending on what they are doing online (e.g. gaming; using an avatar; social media) and why.	I can give examples of how bullying behaviour could appear online and how someone can get support.	I can explain the difference between a 'belief', an 'opinion' and a 'fact. and can give examples of how and where they might be shared online, e.g. in videos, memes, posts, news stories etc.	I can explain why spending too much time using technology can sometimes have a negative impact on anyone; I can give some examples of both positive and negative activities where it is easy to spend a lot of time engaged
YR4	I can give examples of how to be respectful to others online and describe how to recognise healthy and unhealthy online behaviours.	I can explain ways that some of the information about anyone online could have been created, copied or shared by others.	I can explain that others online can pretend to be someone else, including my friends, and can suggest reasons why they might do this.	I can recognise when someone is upset, hurt or angry online.	I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in-app purchases, pop-ups) and can recognise some of these when they appear online.	I can identify times or situations when someone may need to limit the amount of time they use technology e.g. I can suggest strategies to help with limiting this time.
YR5	I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my / our fault.	I can describe ways that information about anyone online can be used by others to make judgments about an individual and why these may be incorrect	I can explain how identity online can be copied, modified or altered.	I can describe the helpline services which can help people experiencing bullying, and how to access them (e.g. Childline or The Mix).	I can evaluate digital content and can explain how to make choices about what is trustworthy e.g. differentiating between adverts and search results.	I can describe some strategies, tips or advice to promote health and wellbeing with regards to technology.
YR6	I can describe how things shared privately online can have unintended consequences for others. e.g. screen-grabs.	I can explain the ways in which anyone can develop a positive online reputation.	I can identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online.	I can describe how to capture bullying content as evidence (e.g screen-grab, URL, profile) to share with others who can help me.	I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how someone might encounter these online (e.g. advertising and 'ad targeting' and targeting for fake news).	I can describe common systems that regulate age-related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose.

Duston Eldean Primary School

'TOGETHER WE GROW'

Appendix 10

Filtering Amendment Log – Staff share-1.Policies folder

Date	Requested by	Details of request	Added by