Eastlea Primary School

Computing and Online Safety Policy

This policy was updated in **March 2026**

Eastlea Primary School Computing and Online safety Policy

This policy should be read in conjunction with other school policies including Anti-Bullying, Behaviour, Staff Health and Well Being, Child Protection, Safeguarding and GDPR.

Introduction

This policy aims to cover the different elements that computing can cover within our school. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum. This policy will set out a framework for how computing will be taught, assessed and monitored throughout the school.

Aims/Rationale

Computing encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for all children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent and independent users and learners of computing we aim:

- To use computing where appropriate to ensure all pupils are motivated and inspired across all areas of the curriculum.
- To use computing to help support all subjects across the curriculum.
- To develop the computing competence, confidence and skills of pupils through computing lessons and provide them with the chance to consolidate these in a cross-curricular context.
- To ensure all pupils are challenged in their use of computing and are provided with exciting, creative ways in which to share their learning.
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use computing to its full potential in all aspects of school life.
- To use computing as a form of communication with parents, pupils and the wider community.

Curriculum

Computing will be taught across the curriculum and wherever possible, integrated into other subjects linked to cross-curricular learning. Discrete sessions will also be used to teach skills that can then be applied in these sessions. The Subject Coordinator will ensure that the plans provide coverage of what is expected as set out in the National Curriculum Programme of Study. They will ensure that all children are challenged and are able to succeed at an appropriate level. In Reception, children will be taught how to use various pieces of equipment, including the computers, in accordance with the curriculum appropriate for them.

Assessment

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during lessons and will be used to inform future planning. Children will also be involved in self and peer assessment to evaluate their own progress and learning. Children will store their work in a variety of ways including on the network in their own documents folder, seesaw portfolios and classroom files.

Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the computing curriculum throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to fulfil their potential.

Roles and Responsibilities - Senior Management Team

The head teacher and other members of the senior management team are responsible for monitoring the teaching throughout the school. The senior management team should decide on the provision and allocation of resources throughout the school in accordance to the school development plan, computing action plans and timescales. They should also ensure that the subject coordinator and teachers are following their roles as listed below and in accordance to job specifications and appraisal targets.

Roles and Responsibilities – Computing Coordinator

The Computing Coordinator will oversee planning in all year groups throughout the school and be responsible for raising standards. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The Subject Coordinator is responsible for managing equipment and providing guidance for future purchasing.

Roles and Responsibilities - Staff

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan, teach and use computing within their class. They will also assist in the monitoring and recording of pupil progress in computing. Teachers should also respond to, and report, any e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures. Online safety training is completed annually by staff and any further updates are shared when needed. Staff should follow, and agree to, the Staff Information Systems Code of Conduct (appendix 1).

Roles and Responsibilities - Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely. If either a visitor or governor wishes to have an account to logon to the school network, they should speak to a member of the senior management team.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and computing can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using computing and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the Computing and Internet agreement (appendix 2). They should ensure that they use the computers and equipment appropriately at all times. It is expected that children will follow the schools behaviour policy when working online. They are also expected to adhere to the schools anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities – Parents / Carers

Parents/Carers should stay vigilant to the websites and content that their children are accessing. They should also talk to their child about e-safety and the use of the internet. If they have any questions or concerns they should speak to their child's class teacher, the subject coordinator or the head teacher.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher and/or subject coordinators. If staff use memory sticks the schools anti-virus software will scan these. Staff should be vigilant to reduce the risks of virus infection. The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher and/or the subject Coordinator for advice. The school reserves the right to examine or delete any files that are held on its system.

Laptops

Staff laptops remain the property of school and must be returned when requested; they are open to scrutiny by senior management, contracted technicians and the subject leader. Laptops belonging to the school must have updated antivirus software installed and be password protected. Staff provided with a laptop purchased by the school are responsible for ensuring updates can be made by the technician as needed. Staff wishing to bring in their personal laptops should clear this in the first instance with either the Online Safety or Computing coordinator. The security of school laptops is of prime importance due to their portable nature and them being susceptible to theft.

iPads

Staff are responsible for ensuring children take care when using the iPads. Staff are unable to download any apps on the iPads and should inform the subject coordinator of any apps they wish to have installed. Children should be reminded of the computing and online safety policy whenever they use iPads.

Network

Staff will be issued with a username for the computer and a password. It is their responsibility to change this in accordance with any password procedures. These accounts will be created and monitored by a Northumberland County Council ICT Technician.

School Website and Online Learning platforms

The school website will be overseen by the head teacher and it is expected that the information located on some pages will be provided by other members of staff and children. Facebook will be updated by nominated staff and photos of children will be only in groups and there will be no names included.

Tapestry and Seesaw are used as online learning platforms throughout school. These posts are monitored by school staff before being approved and added to the children's journals.

E-mail

All members of teaching and support staff will be issued with a school email address and this is the email with which they should use for professional communication. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued.

Internet use, filtering and monitoring

The internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended. The teaching of email and internet use will be covered within the computing curriculum, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet, based around the four C's (see appendix 5 for further information):

- **Content** – what the children see
- **Contact** – who and what they interact with online
- **Conduct** – expectations about online behaviour and also ensuring children know who to talk to if concerned
- **Commerce** – reminder that children may experience scams, phishing and that the algorithms used in games will also be used to target young people with adverts etc

Staff are also aware that the internet provides children and young people with access to a wide-range of content, some of which may include harmful, extremist content. The filtering systems used at our school block inappropriate content, including extremist content. Where staff, pupils or visitors find unblocked extremist content they must report it to the head teacher, Online safety or subject coordinator. Pupils and staff know how to report internet content that is inappropriate or of concern.

All web activity is monitored by the Headteacher, Online Safety and computing coordinator so it is the user's responsibility to ensure they log off appropriately. The use of the internet to access inappropriate materials is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to their teacher or the subject coordinator. The internet and filtering is provided by the local authority who will run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by the local authority.

Online Safety Group

All staff have a responsibility to monitor online safety, filtering and monitoring. Our school Online safety group includes the following stakeholders:

- Designated safeguarding Leads (Emma Beeston, Kay Lister, Vicki Stafford)
- Computing Coordinator (Hannah Betham)
- Online Safety Coordinator (Sarah Atkinson)
- Named Governor for Online Safety (Julie Page)
- IT Support Technician (Dave Mathewson)

Passwords – Password Guidelines

Staff should make sure that any passwords they use are robust and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password. For sites where children have passwords, they will be provided with these by either their teacher or the Subject Coordinator. As children progress through the school they will be taught about choosing sensible passwords.

School Liaison, Transfer and Transition

When a new child joins, it is the responsibility of office staff to inform the subject Coordinator of the child's name and year group. The ICT technician will then provide a network login. Once they have left our school, the child's account will be removed.

Personal Data

Staff should be aware that they should not transfer personal data such as reports, SEND information and contact information on to personal devices unless strictly necessary. This data should then be removed as soon as possible in line with GDPR guidelines.

Social Media

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school.
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening.
- Not use these media to discuss confidential information or to discuss specific children.
- Check with the Subject Coordinator if they need advice on monitoring their online persona and checking their security settings.

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will ensure that we block any followers that appear inappropriate. We will follow guidance laid out in this document to ensure children are kept safe.

Mobile Phones

We are aware that children and young people have access to unfiltered internet when using their mobile phones. This is also referred to in the Computing progression of learning document. Pupils are not allowed to use phones at Eastlea and any that are brought in for a 'one off' reason in KS2 are switched off, handed in to a member of staff for safe keeping and retained until the end of the school day.

Other than in exceptional circumstances staff phones are kept out of sight in the classrooms and only accessed away from the children during breaks/lunchtimes or whilst on visits out of school to maintain communication as part of the risk assessment process. Staff may also use phones at times to upload photos to learning platforms and school social media then immediately delete any photographs from their device.

Artificial Intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative 'chatbots' such as Chat GPT and Google Bard. We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to creates images, audio or video hoaxes that look real. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Digital and Video Images

As regards publishing any photographs or videos of children online, as a school we will aim to ensure that:

- parents or carers have given us written permission.
- children are in appropriate dress and we do not include images of children who are taking part in swimming activities.
- parents/ carers or children can request that a photograph is removed.
- we provide new parents with a images and videos parental consent form upon their arrival into school.
- we ask parents or carers that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online.

Technical Support

Any issues must be logged with the subject coordinator and will then be dealt with by the Technician as soon as possible. Outcomes will be recorded next to the issue. It is a staff member's responsibility to log any issues. Additional office-based support (e.g. SIMs) is provided by the Northumberland County Council IT Helpdesk and forms part of the annual Service Level Agreement that the school has in place.

E-safety incidents – specific procedures

- E-safety rules will be posted in the Computer suite and discussed with the pupils at the start of each year, but reminded that this is an on-going area to consider
- Pupils will be informed that network and Internet use will be monitored through SENSO.
- Complaints of Internet misuse will be dealt with by the head teacher or senior staff, following agreed county procedures (see appendix 3)
- Any complaint about staff misuse must be referred to the head teacher or where the head teacher is involved to the Chair of Governors.
- Safeguarding complaints must be dealt with in accordance with school child protection procedures.
- Discussions will be held with the Police where necessary to establish procedures for handling potentially illegal issues.
- We access and use NCC internet which is covered by Fortinet filtering and monitor the use of websites regularly.

H Betham (Computing Coordinator) and
S Atkinson (E-safety Coordinator)

Appendix 1 -

Eastlea Primary School – Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Computing and E-safety policy (available electronically on the school website) for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will use my individual log-on credentials to access the school computers and not leave computers logged on and unattended.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely and will use a data encrypted memory pen in line with GDPR policies.
- I will take responsibility for the security of any school owned device or information systems that I remove from the school site – this includes physical security from harm such as, but not limited to, theft or vandalism that can be avoided by taking reasonable measures.
- I will take responsibility for keeping any school owned device or information systems secure from unauthorised access by others (such as family members, friends or any others not accepted by the school as having access rights).
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Safeguarding lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I take personal responsibility for the physical security of any device I bring into school or on school visits and I understand that I should not access the internet using any personal device during lesson time or when I am supervising pupils.
- I take personal responsibility for following the protocols outlined in the Computing and E-Safety policy linked to the responsible use of social media.
- I understand that photos may appear on online platforms and media linked to my role in school.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct
Signed: …….. Print name: ……..

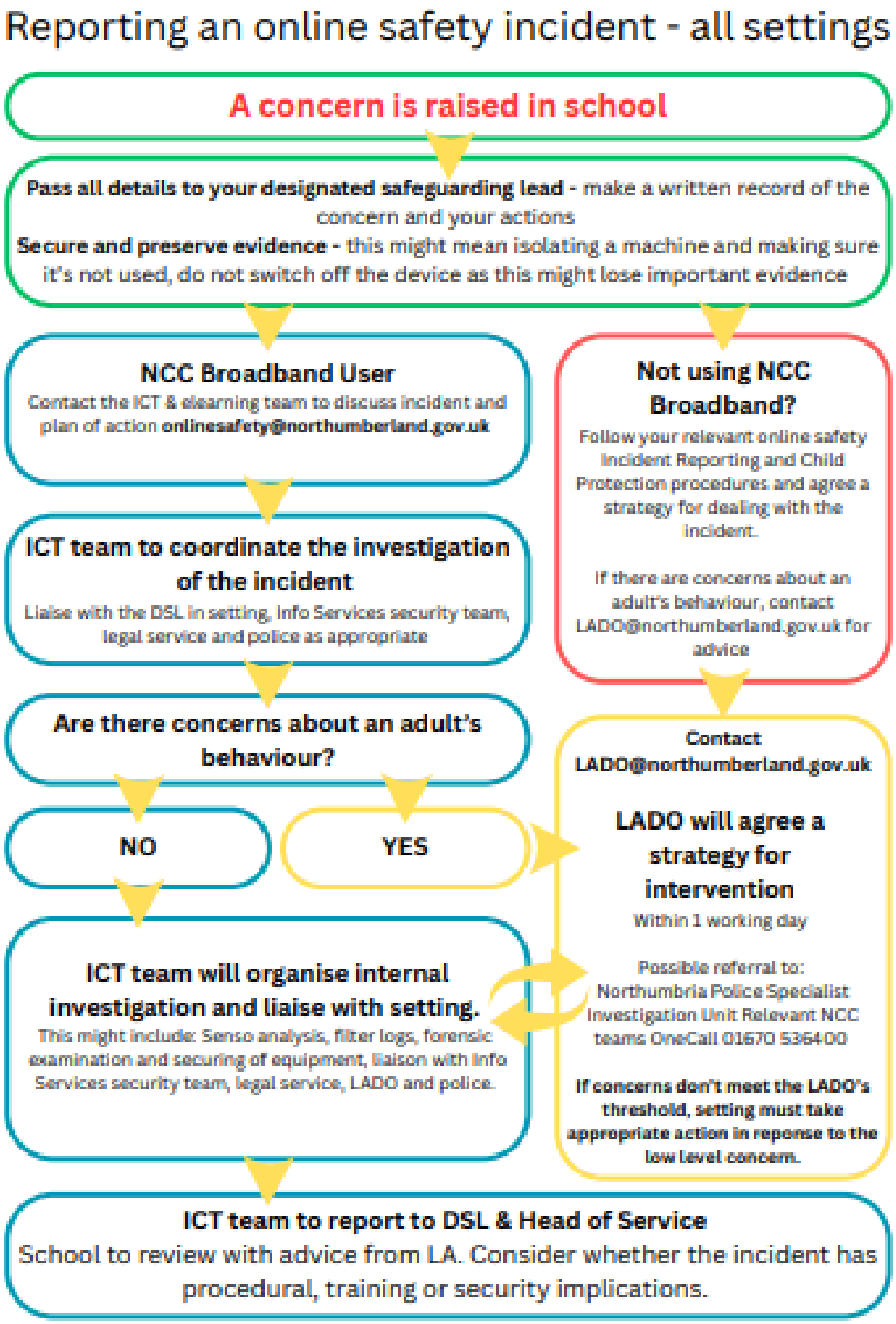
Date: …….. Accepted for school: ……

Appendix 2 –

Eastlea Primary School Computing and Internet Acceptable Use Policy

- I am responsible for what I use the internet for and follow rules to keep me safe.
- If I see something I do not like I will tell an adult straight away as I know they look at what I use the computer for.
- I know I need to keep my password safe and not share it with anyone else.
- I will keep my own and other peoples personal information safe.
- I will use the computers sensible and only access the websites I am told to.
- I know if I don't follow the rules I will not be allowed on the computers.

Appendix 3 -


Reporting an online safety incident - all settings
A concern is raised in school
Pass all details to your designated safeguarding lead - make a written record of the concern and your actions
Secure and preserve evidence - this might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence
NCC Broadband User
Contact the ICT & elearning team to discuss incident and plan of action onlinesafety@northumberland.gov.uk
Not using NCC Broadband?
Follow your relevant online safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.
If there are concerns about an adult's behaviour, contact LADO@northumberland.gov.uk for advice
ICT team to coordinate the investigation of the incident
Liaise with the DSL in setting, Info Services security team, legal service and police as appropriate
Are there concerns about an adult's behaviour?
NO
YES
Contact LADO@northumberland.gov.uk
LADO will agree a strategy for intervention
Within 1 working day
Possible referral to: Northumbria Police Specialist Investigation Unit Relevant NCC teams OneCall 01670 536400
If concerns don't meet the LADO's threshold, setting must take appropriate action in reponse to the low level concern.
ICT team will organise internal investigation and liaise with setting.
This might include: Senso analysis, filter logs, forensic examination and securing of equipment, liaison with Info Services security team, legal service, LADO and police.
ICT team to report to DSL & Head of Service
School to review with advice from LA. Consider whether the incident has procedural, training or security implications.

Appendix 4 –

Dear Parent/Carer,

Images and videos parental consent form

National guidelines for data protection which came into effect from May 2018 involved changes in national legislation to enhance the previous laws which ensure that all data is kept as safely as possible and is only retained and used with consent of those involved. We therefore need to confirm your consent for us to use images and video footage of your child(ren) in school for anything that is above and beyond the normal practice of education/teaching and learning (for which, as before, no consent is required). We are also seeking to simplify the permissions we have previously sought to make things clearer for parents and staff.

There is still quite a lot of information included in this letter and it is rather wordy, but we have to ensure that we are meeting the higher expectations of GDPR.

This form explains the reasons why and how Eastlea Primary may use images and videos of your child(ren).

A copy of this letter is provided for all Eastlea pupils. **Please read the form thoroughly and outline your agreement as appropriate and return to school asap.**

Why do we need your consent?

Eastlea Primary School requests the consent of parents/carers to use images and videos of their child(ren) for a variety of different purposes.

Without your consent, the school will not use images and videos of your child(ren). Similarly, if there are only certain conditions under which you would like images and videos of your child(ren) to be used, the school will abide by the conditions you outline in this form.

Why do you we use images and videos of your child?

Eastlea Primary School uses images and videos of pupils as part of school displays to celebrate school life and pupils' achievements, to promote the school on the school's website, to share updates on the school Facebook page and for other publicity purposes such as news media.

Where the school uses images of individual pupils, the full name of the pupil **will not** be disclosed. Where an individual pupil is named in a written publication, a photograph of the pupil **will not** be used to accompany the text.

Who else uses images and videos of your child?

It is common that the school is visited by local media and press, who take images or videos of children taking part in school events and activities. Images of pupils posted on the school's website/Facebook page may also be shared and used by others who access these platforms, e.g. workshop providers, other schools who take part in shared events with Eastlea.

If any organisations other than those above intend to use images or videos of your child in any other ways, **additional consent** will be sought before any image or video is used.

What are the conditions of use?

- This consent form is valid from **when it is returned until your child leaves Eastlea.**
- It is the responsibility of parents/carers to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not use the personal details or full names of any pupil in an image or video, on our website, on the school Facebook page or any other printed publications.
- The school will not include personal emails, postal addresses or telephone numbers on images or videos on our website, in printed publications.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may use work created by pupils.
- The school may use group or class images or videos with general labels, e.g. 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e. it would not be suitable to display an image of a pupil inappropriately clad in swimwear.
- The school will invite professional photographers to take individual images of your child/family groups which are available to purchase annually. Separate permission is asked for your child to be included on class photos taken by professional photographers each year.

Refreshing your consent

- This form is valid from **when it is returned until your child leaves the school.**

Consent will be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account which will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent

Parents/Carers have the right to withdraw their consent at any time. Withdrawing your consent will not affect any images or videos that have been shared prior to withdrawal.

If you would like to withdraw your consent, you must submit your request in writing to the Head Teacher. Further copies of this form can be obtained from the school office.

We are happy to discuss any further queries you may have about GDPR or consent for use of photos/images in school. These questions can either be addressed to Miss Beeston (Head Teacher) or to Mrs Atkinson (Eastlea E-safety Coordinator). We ask for your support with helping us to continue to adhere to the requirements of national legislation.

Thank you,
Miss E Beeston and Mrs S Atkinson

Eastlea Primary: Images and videos parental consent form

School Communication systems such as **Parentmail**, **Tapestry** and **Seesaw** will be used to send you reminders, updates about school events, advance notice of dates for the diary, reminders about payments that are owed etc.

In addition to this, the school will **only** publish images and videos of your child(ren) for the conditions that you provide consent for. Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria. Then return this form to school as soon as possible.

Name of pupil:	
Class:	

I provide consent to:	**Yes**	**No**
Using images of my child on Facebook and the school website.		
Using images of my child in the class photos taken annually by a professional photographer, usually in the summer term.		

Declaration

I, _____ (name of parent/carer), understand:

- Why my consent is required.
- The reasons why **Eastlea Primary School** uses images and videos of my child.
- Which other organisations may use images and videos of my child.
- The conditions under which the school uses images and videos of my child.
- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with my requirements.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the **Head Teacher**.

Name of parent/carer: _____

Signature: _____

Date: _____

Appendix 5 –

Content – what the children see
Contact – who and what they interact with online
Conduct – expectations about online behaviour and also ensuring children know who to talk to if concerned
Commerce – reminder that children may experience scams, phishing and that the algorithms used in games will also be used to target young people with adverts etc (e.g. if they play a game with gambling in it they may receive ads/ emails about other gambling – just like when we as adults use a search engine for something we find our inbox full of ads and emails about similar products!)
Page 35 para 136 describes in more detail

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

What do you do to protect from harmful content?

Answers:

•Firewalls/Filters
•Teaching about different platforms.

Contact: being subjected to harmful online interaction with other users; for example: child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
What can we do to protect young people?

Answers:

- Create safe spaces for children to talk about their worries.
- Early identification for early help.
- Support parents to engage and talk with their children.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

What can we do to support young people to use mobile technology safely?

Answers:

- Create safe spaces for children to talk about their worries.
- Teach about technology and the law.
- Build resilience and discuss the pros and cons of the use of apps
- Don't be too judgmental, remember this is the young people's world!. Be clear that you can be accessed as support if things go wrong.

Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

What can we do to protect children and young people from commerce risks?

Answers –

- Education about addiction and what this can look like online.
- Support children and young people to develop awareness of how this can impact on them.
- Support parents and carers to monitor online usage and how to disable settings which requires in app purchases.