Online Safety Policy

Designated Safeguarding Lead (s): Karen Burton, Headteacher / Tina Arckless, Pastoral care.

Named Governor with lead responsibility: Rachel Raynor

Link Governor for Computing	Mrs K Peace
Computing Lead and technical support	Danielle Hamilton / Esteem ICT manager - Adrian Foster

Approved by:	K.Burton	**Date:**	September 2023
Last reviewed on:	September 2023		
Next review due by:	September 2024		

Record of Policy Amendment / History

Version/ Issue	Date	Author	Reason for Change
Version 1	Sept 2022	The Key / DHamilton	-
Version 2	June 2023		Update ISP / filtering supplier, staff roles & flowchart.
Version 3	Sept 2023		KSIE updates – filtering and monitoring: Section 3 & 7 Safeguarding policy updates - Section 6.3 & 6.4

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure. **Latest update links to KCSIE**

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

As part of our commitment to online safety, as a school we are using the 360 SAFE audit tools to make constant improvements and work towards accreditation.

Why online safety?

Online safety is the generic term that refers to raising awareness about how children, young people and adults can protect themselves when using digital technology and in the online environment. Child abuse in all its forms is increasingly being linked to the use of digital media. Technology is constantly being updated and the internet can now be accessed via mobile phones, laptops, computers, tablets, webcams, cameras, games consoles and devices (https://derbyshirescbs.proceduresonline.com/p_esafety.html)

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk as defined by KCSIE 2023:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer 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
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation and links to the DDSCP Online Safety and Internet Abuse guidance.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and the Meeting digital and technology standards in schools and colleges government guidance.

3. Roles and responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that 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.

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.All governors will:

  - Ensure that they have read and understand this policy.
  - Agree and adhere to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
  - Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead – Karen Burton / Tina Arkless

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school in collaboration with the Computing co-ordinator (**Danielle Hamilton**), in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ESTEEM ICT Team and computing co-ordinator to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT Team and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety in liaison with the Computing lead (appendix 2 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board – this includes monthly reports generated on Securly.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- This list is not intended to be exhaustive.

3.5 The Esteem ICT Technical Support Staff – Adrian Foster

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and internet (appendix 1) and ensuring that pupils follow the school's terms on acceptable use by displaying the A3 poster in class. (See separate policy)

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, supported by the DSl and Computing lead.
- Being aware of how to report any incidents of those systems or processes failing by discussing them immediately with DSL/DDSL or Computing Lead, using MyConcerns to report and following any actions/advice as necessary.
- Following the correct procedures by putting in a request via email to the DSL / Computing Lead if they need to bypass the filtering and monitoring systems for educational /work purposes.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- All digital communication with pupils 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.
- Implement current policies with regard to the use of digital technologies, mobile devices, cameras etc in lessons.
- In lessons where internet use is pre-planned, pupils 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.
- The reporting flowcharts contained within this online safety policy are to be understood and displayed in classrooms.

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (**See separate Acceptable Use policy for parents and pupils**)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Educating pupils about online safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the

school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

At Elmsleigh Nursery and Infant School, online safety will be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE and is regularly revisited. As a school we use PROJECT EVOLVE to support this (see appendix 5).
- Key online safety messages are reinforced as part of a planned program of assemblies and theme weeks (See appendix 5)
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are helped to understand the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- 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 pupils 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.

See Appendix 4 for further information on progression of skills linked to online safety at Elmsleigh School.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home e.g termly online safety newsletter, and in information via our website or DOJO This policy will also be shared with parents.

Online safety will also be covered during evenings/workshops throughout the year.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DDSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will take place during Computing and PSHE as well as any other time which is appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DDSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or

- Commit an offence.

If inappropriate material is found on the device, it is up to the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / Safeguarding policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

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 ChatGPT 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 create images, audio or video hoaxes that look real. We will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and so are not currently used with children in school.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreement for staff in appendix 1.

7.1 Classroom Use

Elmsleigh Infant and Nursery School uses a wide range of technology. This includes access to:

- Computers, laptops, ipads and other digital devices
- Internet which includes search engines and educational websites
- Learning platforms – Dojo, PurpleMash, BusyThings
- Email through PurpleMash platform and Office 365 for staff
- Games consoles and other games-based technologies
- Web cams

- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Use age-appropriate search tools such as 'Google safe search' or 'CBBC safe search' following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability -
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

7.2 Filtering

- Our ISP is Primary ICT – this is used across the Esteem Trust.
- We use '*Securly*' for our filtering system (https://www.securly.com/filter) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with *Securly* to ensure that our filtering policy is continually reviewed.

If children discover unsuitable sites or images:

- Child to click on the 'Red Button' when using Chrome boxes or close the screen on a Chromebook and inform a member of staff immediately.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or Online Safety lead.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.
- Staff will receive yearly training on the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

7.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - Physical monitoring (supervision by an adult),
  - Reviewing the logfile information though monitoring *Securly's* filtering site.

- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Security and Management of Information Systems

At Elmsleigh Infant and Nursery School we understand the importance of cyber security. We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar emails / attachments.
- Users are aware of 'phishing' emails.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all but the youngest users. (Early Years and Foundation Stage children and some learners with SEND)
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Users are given a copy of the National Cyber Security Centre (NCSC) 'cyber security information cards for schools'
- Staff have yearly refreshers and complete the NCSC's cyber security training – 30-minute training video.

7.5 Managing the Safety of our Website and Online Platforms

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.
- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.6 Managing Email

- Access to our email system (Office 365) will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the community will immediately tell Karen Burton (Headteacher/DSL) or Tina Arckless (Deputy DSL) if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Computing lead, ICT technician, School business manager and Communications and Office Co-ordinator all have admin access to office 365.
- We have a dedicated email for each class enabling parents to contact the class teacher. Parents can also email our school enquiries.

7.7 Use of Videoconferencing and/or Webcams

- We recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites. Elmsleigh school uses Microsoft LifeCam HD-3000.
    - Videoconferencing contact details will not be posted publicly.
    - Webcam equipment will not be taken off the premises.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Any videoconferences will **not** be recorded.
    - We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.
    - See separate Remote Learning Policy and online learning protocols

7.8 Management of Learning Platforms

Elmsleigh Infant and Nursery uses PURPLEMASH as a learning platform.

- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use
- All users will be mindful of copyright and will only upload appropriate content
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - Any material deemed to be inappropriate or offensive will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.

7.9 Management of Applications (apps) used to Record Children's Progress

- We use 'Insight', 'Tapestry' and 'DOJO' to track learners progress and share appropriate information with parents and carers.

- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

- To safeguard learner's data:
    - Only school issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

7.9 Social Media

The expectations' regarding safe and responsible use of social media applies to all members of Elmsleigh Infant and Nursery school community.

- We will control staff access to social media in line with our AUP policy.
- Concerns regarding the online conduct of any member of the Elmsleigh school community on social media, should be reported to the DSL/DDSL and will be managed in accordance with our staff conduct policies.

As an Infant school, learners will be advised:

- About the inappropriateness of accessing social media / online gaming if they are under the age of 13.
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- How to create and use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate resources.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Elmsleigh Infant and Nursery School official social media channels are: ***Facebook pages - 'Elmsleigh Infant and Nursery School' official group page and 'Friends of Elmsleigh' Fundraising group***

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

- The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
- Leadership and selected staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence:

  - Karen Burton (Headteacher)
  - Ellen Collins (Deputy head)
  - Laura Mansfield (Assistant Head)
  - Ruth Samme (School Business Manager)
  - Elisha Flamson (Communications and Office Co-ordinator)
  - Danielle Hamilton (Computing Lead)

- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage any official social media channels.
  - Official social media sites are suitably protected and linked to our website.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving learners will be moderated possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

8. Using mobile devices in school

Elmsleigh Infant and Nursery School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

- Pupils may not bring mobile devices into school without agreement from the headteacher, this will only be in exceptional circumstances. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.
- Members of staff will refer to and adhere to the schools acceptable use policy and any other policy where the staff use of personal devises and mobile phones is referred to.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Regularly re-starting the device to ensure operating systems, anti-virus and anti-spyware software remain up to date.
- Not using memory sticks

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the Computing co-ordinator or DSL.

10. How the school will respond to issues of misuse

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

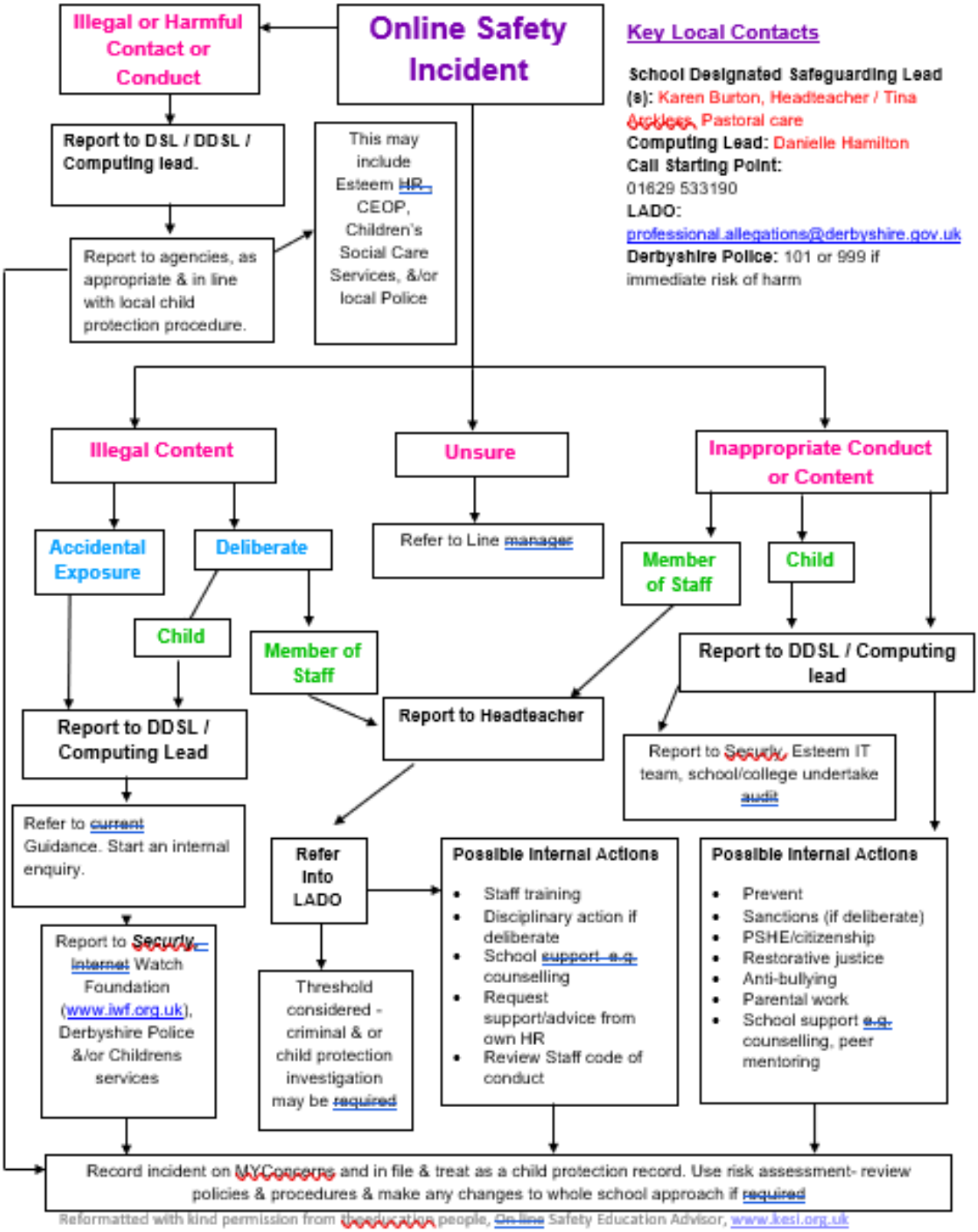
Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police – **see flowchart below for procedures and Appendix 6.**

Responding to an Online Safety Concern

Sept 23 updated



Reformatted with kind permission from theeducation people, On line Safety Education Advisor, www.kesl.org.uk

Version 2.2020. DP CPM Schools/Education

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy will regularly undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DDSL logs behaviour and safeguarding issues related to online safety in liaison with the computing coordinator. An incident report log can be found in appendix 3.

This policy will be reviewed at least yearly by the Computing coordinator in conjunction with the DSL/DDSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures / Professional protocol for Elmsleigh staff
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use

Appendix 1: Acceptable use agreement for staff, governors, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 3: Online safety incident report log *(also to be logged on MyConcern)*

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 4: Online Safety: Progression of skills

This document links to the EYFS Framework 2021, National Curriculum 2014 and the government document 'Education for a connected world' 2020 edition.
Online safety is taught through explicit lessons using PurpleMash platform, discreet teaching through PSHE and PROJECT EVEOLVE and 'Online safety days' / whole school online safety weeks.

	Year group - skills		
Curriculum objective	Nursery / Reception	Year 1	Year 2
Personal, Social and Emotional Development ELG Be confident to try new activities and show independence, resilience and perseverance in the face of challenge; Explain the reasons for rules, know right from wrong and try to behave accordingly. Expressive Arts and Design ELG Safely use and explore a variety of materials, tools and techniques, experimenting with colour, design, texture, form and function.	Recognise purposes for using technology in school and at home. Understand that things they create belong to them and can be shared with others using technology. Recognise that they can use the internet to play and learn. Talk about good and bad choices when using websites – being kind, telling a grown up if something upsets us & keeping ourselves safe by keeping information private.		
Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.		Children understand the importance of keeping information, such as their usernames and passwords, private and actively demonstrate this in lessons. Children take ownership of their work and save this in their own private space such as their My Work folder on PurpleMash.	Children know the implications of inappropriate online searches. Children begin to understand how things are shared electronically such as posting work to the PurpleMash display board. They develop an understanding of using email safely by using 2Respond activities on PurpleMash and know ways of reporting inappropriate behaviours and content to a trusted adult.

Self-image and identity	I can recognise that I can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset. I can explain how this could be either in real life or online.	I can recognise that there may be people online who could make me feel sad, embarrassed or upset. 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.	I can explain how other people's identity online can be different to their identity in real life. I can describe ways in which people might make themselves look different online. I can give examples of issues online that might make me feel sad, worried, uncomfortable or frightened; I can give examples of how I might get help.
Online relationships	I can recognise some ways in which the internet can be used to communicate. I can give examples of how I (might) use technology to communicate with people I know.	I can use the internet with adult support to communicate with people I know. I can explain why it is important to be considerate and kind to people online	I can use the internet to communicate with people I don't know well (e.g. email a pen pal in another school/ country). I can give examples of how I might use technology to communicate with others I don't know well.
Online reputation	I can identify ways that I can put information on the internet.	I can recognise that information can stay online and could be copied. I can describe what information I should not put online without asking a trusted adult first.	I can explain how information put online about me can last for a long time. I know who to talk to if I think someone has made a mistake about putting something online.
Online bullying	I can describe ways that some people can be unkind online. I can offer examples of how this can make others feel.	I can describe how to behave online in ways that do not upset others and can give examples.	I can give examples of bullying behaviour and how it could look online. I understand how bullying can make someone feel. I can talk about how someone can/would get help about being bullied online or offline
Managing online information	I can talk about how I can use the internet to find things out. I can identify devices I could use to	I can use the internet to find things out. I can use simple keywords in search engines. I can describe and demonstrate how to get	I can use keywords in search engines. I can demonstrate how to navigate a simple webpage to get to information I need (e.g. home,

	access information on the internet. I can give simple examples of how to find information (e.g. search engine, voice activated searching).	help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable worried or frightened.	forward, back buttons; links, tabs and sections). I can explain what voice activated searching is and how it might be used (e.g. Alexa, Google Now, Siri). I can explain the difference between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'. I can explain why some information I find online may not be true.
Health, wellbeing and lifestyle	I can identify rules that help keep us safe and healthy in and beyond the home when using technology. I can give some simple examples	I can explain rules to keep us safe when we are using technology both in and beyond the home. I can give examples of some of these rules.	I can explain simple guidance for using technology in different environments and settings. I can say how those rules/guides can help me.
Privacy and security	I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location). I can describe the people I can trust and can share this with; I can explain why I can trust them.	I can recognise more detailed examples of information that is personal to me (e.g. where I live, my family's names, where I go to school). I can explain why I should always ask a trusted adult before I share any information about myself online. I can explain how passwords can be used to protect information and devices.	I can describe how online information about me could be seen by others. I can describe and explain some rules for keeping my information private. I can explain what passwords are and can use passwords for my accounts and devices. I can explain how many devices in my home could be connected to the internet and can list some of those devices.
Copyright and ownership	I know that work I create belongs to me. I can name my work so that others know it belongs to me.	I can explain why work I create using technology belongs to me. I can say why it belongs to me (e.g. 'it is my idea' or 'I designed it'). I can save my work so that others know it belongs to me (e.g. filename, name on content).	I can describe why other people's work belongs to them. I can recognise that content on the internet may belong to other people.

Appendix 5: ELMSLEIGH INFANT AND NURSERY SCHOOL - Online Safety - whole school sessions overview x 3 per year

National Curriculum objective covered - use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

	AUTUMN 1 – Rules that keep us safe	SPRING 1 -Link to global internet safety week + Privacy and security	SUMMER 2 – Being kind online
ASSEMBLY	staying-safe-on-the-internet PPT AUT 1 Send out info to parents – 0-5 guide and 6-10 guide		Choose-kindness PPT SUM 2 All children to be sent home with a 'digital wellbeing' leaflet.
NURSERY	Who uses a tablet / ipad / laptop / phone / computer? Learn the 'Use Your Tablet Safely' Song and talk about what we can do to stay safe when using a tablet. Adults should always know.		Focus on being kind to others – create a class 'advice' poster with post-its and pictures of how to be kind.
RECEPTION	<u>Education for a Connected World:</u> <u>Self-image and identity</u> I can recognise that I can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset. I can explain how this could be either in real life or online. <u>Health well-being & Lifestyle</u> I can identify rules that help keep us safe and healthy in and beyond the home when using technology I can give some simple examples	<u>Education for a Connected World:</u>	<u>Education for a Connected World:</u> <u>Online Bullying</u> I can describe ways that some people can be unkind online. I can offer examples of how this can make others feel. <u>Online Relationships</u> I can recognise some ways in which the internet can be used to communicate. I can give examples of how I (might) use technology to communicate with people I know.
	<u>PSHE</u> Increasingly follow rules, understanding why they are important.	<u>PSHE</u> Be able to manage their own personal needs e.g: sensible amounts of 'screen time'	<u>PSHE</u> Think about the perspectives and feelings of others
	Talk about good and bad choices when using websites – being kind, telling a grown up if something upsets us & keeping ourselves safe by keeping information private Play appropriate games on the internet		

	*Smartie the Penguin PPT B - Pop ups and in app purchasing /Inappropriate websites for older children/Cyberbullying *Smartie the penguin-activity EYFS – cut and stick to make a penguin, then stick on a speech bubble & scribe, ask child what they can do to stay safe when using the internet.		*PROJECT EVOLVE Toolkit – Resources - Year Group - Early Years – Activity 1 - I can describe ways that some people can be unkind online. Activity 2 - I can offer examples of how this can make others feel
YEAR 1	<u>Education for a Connected World:</u> <u>Self-image and identity</u> 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. <u>Health well-being & Lifestyle</u> I can explain rules to keep us safe when we are using technology both in and beyond the home. I can give examples of some of these rules. <u>Managing information online</u> I can describe and demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable worried or frightened.	<u>Education for a Connected World:</u> <u>Privacy and Security</u> I can explain why I should always ask a trusted adult before I share any information about myself online	<u>Education for a Connected World:</u> <u>Online Bullying</u> I can describe how to behave online in ways that do not upset others and can give examples. <u>Online Relationships</u> I can explain why it is important to be considerate and kind to people online <u>Self-image and identity</u> I can recognise that there may be people online who could make me feel sad, embarrassed or upset.
	<u>PSHE</u> R9 Recognising how to ask for help if a friendship is making them feel unhappy. R20. Identifying what to do if they feel worried. H19. Recognising when they need help and understand how to ask for help. L2 Construct and explore the importance of rules.		<u>PSHE</u> R9 Recognising how to ask for help if a friendship is making them feel unhappy R10. Recognising that bodies/feelings can be hurt by words and actions. R11 Identifying how people may feel if they experience hurtful behaviour or bullying. R12 Understanding that hurtful behaviour is not acceptable R21 Identifying what is kind and unkind behaviour. R22 Recognising how to treat themselves and others with respect.

			L7 Explaining how the internet and devices can be used safely to communicate with others
	Talk about good and bad choices when using websites – being kind, telling a grown up if something upsets us & keeping ourselves safe by keeping information private Play appropriate games on the internet		
	* Buddy the Dog's Internet Safety Story PPT – Discuss ways to stay safe online with regards to adverts on games / watching videos / talking to people on the internet *Buddy the dog's internet safety quiz PPT *How To Use a Tablet Safely Activity Sheet – Use examples learnt from PPTs to write/draw how to use a tablet safely. *Create a whole class rules poster for using our ipads.		*PROJECT EVOLVE Toolkit – Resources - Year Group - Year One – Activity 1 - I can describe how to behave online in ways that do not upset others and can give examples. *Cyberbullying - Getting Help Cut and Stick Activity *Cyberbullying -Say No to Cyberbullying Colouring Page
YEAR 2	<u>Education for a Connected World:</u> <u>Self-image and identity</u> I can give examples of issues online that might make me feel sad, worried, uncomfortable or frightened; I can give examples of how I might get help. <u>Health well-being & Lifestyle</u> I can explain simple guidance for using technology in different environments and settings. I can say how those rules/guides can help me.	<u>Education for a Connected World:</u> <u>Privacy and Security</u> I can explain what passwords are and can use passwords for my accounts and devices. I can explain how many devices in my home could be connected to the internet and can list some of those devices. I can describe and explain some rules for keeping my information private.	<u>Education for a Connected World:</u> <u>Online Bullying</u> I can give examples of bullying behaviour and how it could look online. I understand how bullying can make someone feel. I can talk about how someone can/would get help about being bullied online or offline.
	<u>PSHE</u> H28 – Talking about rules and age restrictions that keep us safe H34 - Explaining basic rules to keep safe online		<u>PSHE</u> R11 Identifying how people may feel if they experience hurtful behaviour or bullying R12 Explaining how to report bullying and the importance of telling a trusted adult
	Stay safe online by choosing websites/games that are good for them to visit & not inappropriate e.g age restrictions / adult content	Learn that many websites ask for information that is private & discuss how to responsibly handle such requests	

	*buddy-the-dogs-internet-safety-discussion-cards. After discussion, choose a card and write their answer. *SMART Zoobook Messenger – should parrot share his address? *Design a SMART rules tablet *Discuss online games the children play and the recommended age.		*PROJECT EVOLVE Toolkit – Resources - Year Group - Year Two - Online Bullying - Activity 1 - I can explain what bullying is, how people may bully others and how bullying can make someone feel Activity 3 - I can talk about how anyone experiencing bullying can get help.
RAINBOW ROOM	Choose relevant activities and learning from across the year groups.		

Online safety - Project Evolve coverage

Per half term -

1 Lesson to create knowledge map

1 lesson to address outcomes

Can be in Computing time, PSHE or as a starter to your computing lessons depending on length of lesson needed.

AUT 1	AUT 2	SPR 1	SPR 2	SUM 1	SUM 2
WS - Rules to keep us safe		WS - UK internet safety week			WS - Being kind online
*Online reputation *Copyright & ownership	*Online bullying	*Privacy & security	*Managing online information	*Health & wellbeing *Self-image & identity	*Online relationships

WS - Whole school online safety week focus

Appendix 6: Procedures for Responding to Specific Online Incidents or Concerns

1. Child-on child: Online Sexual Violence and Sexual Harassment between Children

- Elmsleigh Infant and Nursery school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance of 'Keeping children safe in education'.
- We recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and behaviour policies.
- We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and behaviour policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

2. Youth Produced Sexual Imagery ("Sexting")

- Elmsleigh Infant and Nursery School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant safeguarding procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Store the device securely.

- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

3. Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Elmsleigh Infant and Nursery School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available on our website as well as the 'Red Button' on children's devices.

- If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Derbyshire police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

4. Indecent Images of Children (IIOC)

- Elmsleigh Infant and Nursery School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Children Partnership Safeguarding procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the Headteacher is informed in line with our managing allegations against staff policy immediately and without any delay.

- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

5. Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Elmsleigh Infant and Nursery School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Derbyshire police and or the safer Derbyshire website https://www.saferderbyshire.gov.uk/home.aspx

6. Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site and we monitor internet activity. (*Please refer to our Extremism and Radicalisation Policy*).
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire PREVENT pathway which may include a referral into Channel.
- If we are concerned that a member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

7. Harmful Online Challenges and Hoaxes

- If we become aware of any incidents involving online challenges or hoaxes, we will follow the DDSCP Briefing Note: Harmful Online Challenges and Hoaxes guidance.