NEWCOMEN

PRIMARY

SCHOOL

'BELIEVE ACHIEVE SUCCEED'

Online Safety Policy

Designated Safeguarding Lead: Miss Kinga Pusztai (HT)

Designated Deputy Safeguarding Lead: Mr Ed Jones (DHT)

Designated Governor for Safeguarding: Mr Barry Greenwood

Headteacher: ________________________________ **Date:** ___________

Chair of Governors: __________________________ **Date:** ___________

Written by	Kinga Pusztai
Date	September 2024
To Be Reviewed	September 2025

1. Policy Aims

- This online safety policy has been written by Newcomen Primary School involving staff, learners and parents/carers, building on the Kent County Council /The Education People/Durham County Council online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2024, Early Years and Foundation Stage, 'Working Together to Safeguard Children'
- The purpose of this online safety policy is to:
  - Safeguard and protect all members of our school community online
  - Identify approaches to educate and raise awareness of online safety throughout the school community
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
  - Identify clear procedures to use when responding to online safety concerns.
- Our school identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm
  - **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. We will report any concerns to the Anti-Phishing Working Group

2. Policy Scope

- Online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- The internet and associated devices such as computers, tablets, mobile phones and games consoles are an important part of everyday life.
- Learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing board, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

a. Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Acceptable Use Policies (AUP)
- Staff Code of Conduct policy
- Policy to Promote Positive Behaviour
- Child Protection policy
- Child on Child Abuse Policy

  - Curriculum policies, such as: Computing and Relationships Education (RE)
  - Data Protection
  - Searching, Screening and Confiscation policy (DFE)

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. This policy will be reviewed at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns.
- Online safety practice and incidents, including filtering and monitoring processes, will be monitored and reviewed by the Governing Bord.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Kinga Pusztai, has lead responsibility for online safety.
- We recognise that all members of the school community have important roles and responsibilities to play with regards to online safety.
- The Governing Board will ensure online safety is a running and interrelated theme when devising and implementing our whole-school approach to safeguarding. Our safeguarding governor, Barry Greenwood, will monitor this.

a. The school senior leadership team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks. For further detail see DfE guidance on meeting digital and technology standards in schools and colleges.
- Ensure that online safety is embedded within a progressive curriculum which enables all learners to develop an age-appropriate understanding of online safety.
- Support the Headteacher by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

b. **The Designated Safeguarding Lead (DSL) - Headteacher will:**

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSL to ensure online safety is recognised as part of the setting's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour.
- Ensure that online safety is promoted to parents, carers and the wider school community through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Governing Board.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

Keeping Children Safe in Education states that:
"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

c. **Governors:**

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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

d. **It is the responsibility of all members of staff to:**

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues including signposting to appropriate support.
- Take personal responsibility for professional development in this area.
- Know and contribute to the school filtering and monitoring processes.

e. **It is the responsibility of staff managing the technical environment to:**

- Provide technical support and perspective to the Headteacher, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the Headteacher and leadership team to ensure that the setting's IT infrastructure/system is secure and not open to misuse or malicious attack whilst allowing learning opportunities to be maximised.
- Ensure that our filtering and monitoring procedures are applied and updated on a regular basis. Responsibility for its implementation is shared with the leadership team.
- Ensure that our filtering and monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the Headteacher to the filtering and monitoring systems to enable them to take appropriate safeguarding action.

f. It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Read and adhere to the acceptable use policies
- Respect the feelings and rights of others, both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult if there is a concern online and support others that may be experiencing online safety issues.

g. It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies – signed September 2023**.**
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting or other appropriate agencies if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

a. Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Relationships Education (RE) and computing programmes of study.
  - Reinforcing online safety messages whenever technology is being used.
  - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Promoting positive use of technology.

    - Seeking learner voice when writing and developing online safety policies and practices - including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

b. Vulnerable Learners

- We recognise that some learners are more vulnerable online due to a range of factors.
- We will ensure that appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum, we will seek input from specialist staff as appropriate.

c. Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis - with at least annual updates.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

d. Awareness and engagement with parents and carers

- We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering online safety awareness training.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, Twitter and on our website.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education approaches.

7. Safer Use of Technology

a. Classroom Use

- Our school uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - The internet which may include search engines and educational websites
  - Email
  - 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.
- The setting will use appropriate search tools search engines and online tools.
- 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.
  - **Key Stage 2**
    - Learners will use appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners' age and ability.

b. Managing Internet Access

- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

c. Filtering and Monitoring

i Decision Making

- Governors and Leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place to limit learners' exposure to online risks.
- Governors and Leaders are aware of the need to prevent "over blocking" as that may unreasonably restrict what can be taught with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by the Leadership Team. All changes to the filtering policy are logged and recorded.
- 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.

ii Filtering

- Education broadband connectivity is provided through Virgin Media Business**.**
- We use Meraki Firewall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. We also are aware of the filtering detecting other safeguarding issues, such as self-harm, serious violent crime or issues with county lines grooming.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- Content lists are regularly updated
- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges
- All school devices are connected to a filtered feed. If a school device needs access to additional content, for instance to manage official social media, the filter settings for that device or user should be modified to allow access to that content once the headteacher has been consulted.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes
- Any material believed to be illegal will be reported immediately to the appropriate agencies.

iii Monitoring

The school monitors all network use across all its devices and services.

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - Physical monitoring (supervision), monitoring internet and web access.

    - Alerting e-mails are sent to the Headteacher who then takes appropriate action.
- If a concern is identified via monitoring approaches:
    - Headteacher will respond in line with the child protection policy.
- 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.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

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

- physical monitoring
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to Leadership Team

Please refer to Appendix 1 for more information.

d. Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our Data Protection policy.

e. Security and Management of Information Systems

- 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 or access via appropriate secure remote access systems.
    - Not using portable media without specific permission.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.

  - Regularly checking files held on our network.
  - The appropriate use of user logins and passwords to access our network.
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security can be found at: Acceptable use policies that contain other information

f. Password policy

- All members of staff will have their own unique username and private passwords to access our systems. Members of staff are responsible for keeping their password private.
- All learners in KS2 are provided with their own unique username and private passwords to access our systems. Learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Change their passwords regularly
  - Always keep their passwords private.
  - Not to login as another user at any time.

g. Managing the Safety of our Website

- 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 learners' 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.

h. Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices.

i. Managing Email

- Access to our email systems 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 the Headteacher if they receive offensive communication and this will be recorded in our safeguarding files/records.

i **Staff email**

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email.

8. Social Media

a. Expectations

- The expectations regarding safe and responsible use of social media applies to all members of our school community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of our school community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of our school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
    - The use of social media during lesson times for personal use is not permitted.
    - Inappropriate use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action.
- Concerns regarding the online conduct of any member of our school community on social media should be reported to the Headteacher and will be managed in accordance with our appropriate policies.

b. Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct policy and acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the correct privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of our school on their personal social networking accounts. This is to prevent information on these sites from being linked with the setting and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with the Headteacher.
    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the Headteacher.

C. Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age-appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13. Therefore, we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
  - 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.
  - To use safe passwords.
  - To use apps and communication tools 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.

d. **Official Use of Social Media**

- The school's official social media channels are: Twitter (X) and Youtube.
- The official use of social media sites only takes place with clear educational or community engagement objectives.
- 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.
- Official social media use will be conducted in line with existing policies.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Always be professional and aware they are an ambassador for the setting.
  - Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the setting.

- Always be responsible, credible, fair and honest and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Mobile and Smart Technology

- Our school recognises that personal communication through mobile technologies is an accepted part of everyday life but technologies need to be used safely and appropriately within the setting.

a. Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate policies such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- All members of our school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage. We accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of our school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices. Passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community. Any breaches will be dealt with in-line with our policies and procedures.
- All members of our school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.
- All members of our school community are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the discipline policy.

b. Staff Use of Mobile and Smart Technology

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law as well as relevant policy and procedures.

- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Not use mobile phone during teaching periods unless permission has been given by the Headteacher.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are NOT permitted to use their own personal phones or devices for contacting learners or parents and carers. Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher.
- If a member of staff breaches our policy, action will be taken in line with our code of Conduct Policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the police will be contacted.

c. Learners' Use of Mobile and Smart Technology

- Children's mobile phones and personal devices are not permitted to be used in school and must be handed into the office at the start of each day. They can be collected at the end of the day.
- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with the DFE Searching, Screening and Confiscating Guidelines www.gov.uk/government/publications/searching-screening-and-confiscation)
- Learners' mobile phones or devices may be searched by a member of the leadership team with the consent of the parent/carer. Content may be deleted or requested to be deleted if it contravenes the DFE Searching, Screening and Confiscating Guidelines.
- Mobile phones and devices that have been confiscated will be released to parents or carers in person.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

d. Visitors' Use of Mobile and Smart Technology

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with guidance provided to them on their visitor pass.

- Members of staff are expected to challenge visitors if they have concerns and will always inform Headteacher of any breaches our policy.

e. Officially provided mobile phones and devices

- Setting mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies

10. Responding to Online Safety Incidents and Concerns

- 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. The community will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will identify lessons learnt and implement any policy or curriculum changes as required.
- The school will follow the NSPCC guidance on when to contact the Police available here :-

when-to-call-the-police--guidance-for-schools-and-colleges.pdf (npcc.police.uk)

- If an incident or concern needs to be passed beyond our community, the Headteacher will speak with Cleveland Police first to ensure that potential investigations are not compromised.

a. Concerns about Learners' Welfare

- The Headteacher will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The Headteacher will record these issues in line with our Child Protection Policy.
- The Headteacher will ensure that online safety concerns are escalated and reported to relevant agencies in line with the MACH thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

b. Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher in accordance with the Child Protection Policy.
- Issues which do not meet the threshold requiring reporting to the LADO will be recorded by the school in accordance with the Child Protection Policy.

- Any allegations regarding a member of staff's online conduct reaching the threshold will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

a. Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood the guidance and part 5 of 'Keeping children safe in education' 2024
- 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 Policy.
- We recognise that 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 Relationships Education 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 Headteacher and act in accordance with our child protection and anti-bullying 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 school policies.
  - Inform parents and carers about the incident and how it is being managed.

  - If appropriate, make a referral to partner agencies.
  - 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 Headteacher will discuss this with Cleveland 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.

Youth Produced Sexual Imagery ("Nudes")

- We recognise youth produced sexual imagery (known as "nudes") as a safeguarding issue. All concerns will be reported to and dealt with by the Headteacher.
- This section only applies to YP under the age of 18 creating/sharing/receiving nudes of a YP. It does not apply to children sharing adult pornography.
- On any occasion when an adult is in possession of or is sharing an illegal image of a YP – this will always be an urgent police matter.
- We will follow the advice set out by the DfE https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- 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 review the handling of any incidents to ensure that best practice was implemented.

b. Online Child Sexual Abuse and Exploitation

- We 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 Headteacher.
- Schools are reminded that a criminal offence has been committed if a person aged 18 or over intentionally communicates with a child under 16, who the adult does not reasonably believe to be 16 or over, if the communication is sexual or if it is intended to encourage the child to make a communication which is sexual. The offence will be committed whether or not the child communicates with the adult. This is the offence of sexual communication with a child under section 67 of the Serious Crime Act 2015.

- 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.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. If made aware of incident involving online child sexual abuse and we will:
    - Act in accordance with our child protection policies.
    - If appropriate, store any devices involved securely.
    - Make a referral to Mach (if required/appropriate) and immediately inform Cleveland 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 Headteacher will obtain advice immediately through the Mach or Cleveland Police.
- If learners at other settings are believed to have been targeted, the Headteacher will seek support from Cleveland Police to ensure that potential investigations are not compromised.

c. Indecent Images of Children (IIOC)

- We 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 Headteacher will obtain advice immediately through the Mach or Cleveland Police.
- If made aware of IIOC, we will:
    - Act in accordance with our Child Protection Policy.
    - Store any devices involved securely.

    - Immediately inform appropriate organisations.
- 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 Headteacher 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 Headteacher 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 Police via 101 (999 if there is an immediate risk of harm) and First Contact
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) if 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.
    - 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.

d. Child Criminal Exploitation – Including County Lines

- All staff need to be aware of the indicators that a child may be at risk from, or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology.

e. Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at our school.
- Full details of how we will respond to cyberbullying are set out in our behaviour policy.

f. Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at our school and will be responded to in line with existing policies.

- 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 Headteacher will obtain advice through the Mach or Cleveland Police

g. 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 via our robust filtering and monitoring system.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with our Child Protection Policy.
- If we are concerned that 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.

12. Useful Links for Educational Settings

National Links and Resources for Educational Settings:

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Parentzone (Google Internet Legends) https://parentzone.org.uk/

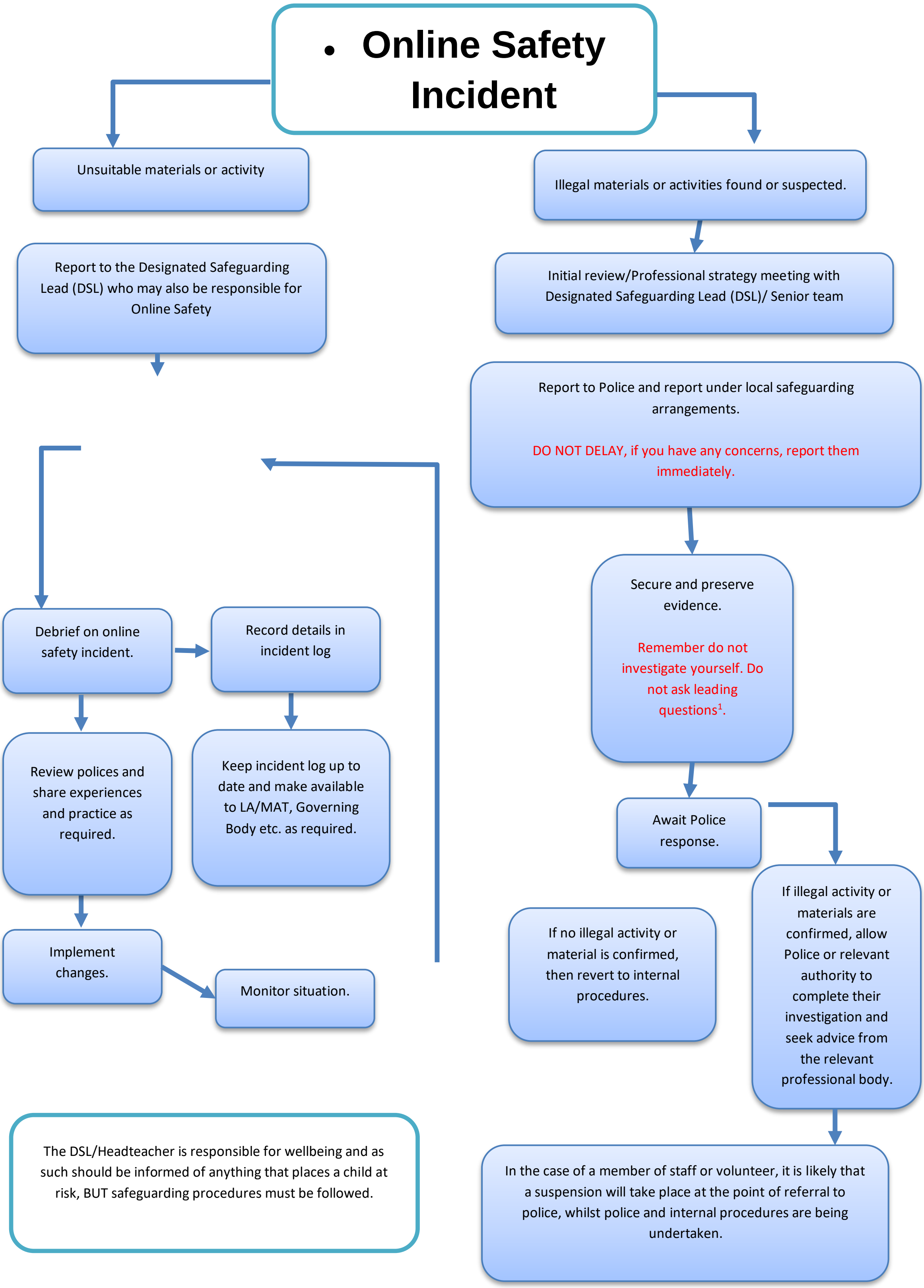
National Links and Resources for Parents/Carers:

- Internet Matters: www.internetmatters.org

This site is particularly useful for providing clear information and up-to-date advice on setting parental controls.

- Action Fraud: www.actionfraud.police.uk (This is the place to report ransomware, scams etc.)

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- Parent protect - advice for parents having difficulties e.g. Peer on peer abuse or Police involvement www.parentsprotect.co.uk/
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk



- **Online Safety Incident**

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

Debrief on online safety incident.

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes.

Monitor situation.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response.

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix

1

Filtering and Monitoring Guidelines

NEWCOMEN

School Filtering and Monitoring Guidelines

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system". However, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

What is filtering and monitoring?

Filtering systems block access to harmful websites and content. Monitoring systems identify when someone searches for or accesses certain types of harmful online content on school devices, identify who is searching for or accessing the harmful content and alerts the school about it so we can intervene and respond

Responsibilities - We're all responsible for filtering and monitoring

No filtering and monitoring software is perfect as it might not be aware of all the websites that contain inappropriate content, abbreviations or misspellings in a search engine may slip past the software, inappropriate content may be found on websites considered 'safe'.

Governors and Leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks. They are also aware of the need to prevent "over blocking" as that may unreasonably restrict what can be taught with regards to online activities and safeguarding.

The management of the school's filtering policy is overseen by the Network Manager with support from the Senior Leadership Team. He manages the school filtering and will keep records of breaches of the filtering systems. The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be approved by the headteacher. All users have a responsibility to report immediately to the headteacher of any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

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 essentials

Filtering and Monitoring

Filtering

Education broadband connectivity is provided through Virgin Media Business**.** We use Meraki Firewall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. We also are aware of the filtering detecting other safeguarding issues, such as self-harm, serious violent crime or issues with county lines grooming. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list. All school devices are connected to a filtered feed.

Changes to the Filtering System

If a school device needs access to additional content, for instance to manage official social media, the filter settings for that device or user should be modified to allow access to that content once the headteacher has been consulted.

- Staff member observes site that is unavailable.
- Staff member obtains filtering log request form from Network Manager.
- Staff fill in form with full details of the site that requires unblocking.
- The form is then passed back to the network Manager.
- The Network Manager checks the site and passes the form onto the Headteacher for approval and a signature to authorise unblocking/blocking of the site.
- The completed form is filed in the Network Manager's office as evidence.
- Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the class teacher who will report the matter to the Headteacher.

Monitoring

We will appropriately monitor internet use on all setting internet enabled devices. This is achieved by: Physical monitoring (supervision), monitoring internet and web access. Alerting e-mails are sent to the Headteacher who then takes appropriate action. If a concern is identified via monitoring approaches, the Headteacher will respond in line with the child protection policy. 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. Any material believed to be illegal will be reported immediately to the appropriate agencies.

If learners discover unsuitable sites, they will be required to:

1. Turn off monitor/screen and report the concern immediate to a member of staff.
2. The member of staff will report the concern to the Headteacher
3. The breach will be recorded and escalated as appropriate.
4. Parents/carers will be informed of filtering breaches involving their child.

Inappropriate content includes:

Illegal content (e.g. child sexual abuse), discriminatory content (e.g. sexist, racist or homophobic content), sites that promote drugs or substance abuse, extremist content (e.g. the promotion of terrorism, gambling sites, malware and/or hacking software, pornography, pirated material (copyright theft, sites that promote self-harm, suicide and/or eating disorders and violent material,

Education / Training / Awareness

Pupils are made aware of the importance of filtering systems through the school's online safety curriculum. They are also warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through signing the Acceptable Use Policy and Staff Training. Parents are informed of the school's filtering policy through the Acceptable Use agreement and through ParentMail and online safety session with Online Safety experts.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *The Headteacher / Deputy Headteacher / Safeguarding Governor*

Appendix

2

Searching, Screening and Confiscation Incident Report Sheet

NEWCOMEN

Newcomen Primary School

Searching, Screening and Confiscation Incident Report Sheet

Searching can play a critical role in ensuring that Newcomen Primary is a safe environment for all pupils and staff. It is a vital measure to safeguard andpromote staff and pupil welfare, and to maintain high standards of behaviour through which pupils can learn and thrive. The Headteacher and staff are authorised to have a statutory power to search a pupil or their possessions where they have reasonable grounds to suspect that the pupil may have a prohibited item

Date, time and location of the search:

Name of pupil searched:

Who conducted the search and any other adults or pupils present:

What was being searched for:

The reason for searching:

What items, if any, were found:

Person completing form:
Date and Signature

Headteacher:
Date and Signature

Action Taken	**By whom**	**Outcome**

Appendix

3

Online Incident Report Sheet

NEWCOMEN

Newcomen Primary School

Positive Relationships and Respectful Behaviour to all Members of our School Community

Online Safety Incident Report Sheet

Name of child / children:
Date:
Website accessed:
Nature of incident

Person completing form: Date and Signature	
Headteacher: Date and Signature	
Seen by network manager? Date and Signature	

Action Taken	**By whom**	**Outcome**