



Online Safety Policy

Our Shared Vision

At Becontree Primary School we have **high expectations** of all members of our school community. We **value** the efforts of all and work to enable everyone associated with the school to fulfil their potential and **contribute positively** to their educational experiences. Our school motto '**Respecting One Another**' includes showing respect for ourselves and others.

Equality Mission Statement

We are committed to ensuring equality of educational opportunity and support for all children, parents, carers, staff and visitors irrespective of age, sex, race, disability, religion or belief, sexual orientation, pregnancy, gender reassignment, and socio-economic background. We aim to provide a fully inclusive school in which every person feels proud of their identity and is able to participate fully within the school community. We believe that a diverse school community is a strength which should be respected and celebrated by all those who learn, teach and visit here.

Approved by: FGB	Date: 11.12.25
Signature (Chair of Governors): Signed copy held in file	Signature (Headteacher): Signed copy held in file

Last reviewed on: November 2025	Next review date: November 2026
--	--

Based on documents from:

South West Grid for Learning (SWGfL)

London Grid for Learning (LGfL)

Barking and Dagenham School Improvement Partnership (BDSIP) for London Borough of Barking and Dagenham (LBBD)



This policy covers many of the articles from the UN Convention on the Rights of the Child. Some key ones are listed below.

Article 3

All organisations concerned with children should work towards what is best for each child.

Article 13

Every child must be free to express their thoughts and opinions and to access all kinds of information, as long as it is within the law.

Article 17

Every child has the right to reliable information from a variety of sources. Information should be provided in a way children can understand. Children must be protected from materials that could harm them.

Article 19

Governments should ensure that children are properly cared for and protect them from violence, abuse and neglect by their parents, or anyone else who looks after them.

Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. It is designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Online Safety Policy Review

The school's Online Safety Policy will operate in conjunction with other policies including Safeguarding, Behaviour and Attitudes, Anti-Bullying, Peer on Peer policy, Staff Code of Conduct, Computing, RSHE (Relationships Education, Relationships and Sex Education and Health Education) and PSHE (Personal, social, health and economic) curriculum, GDPR Policy and any Home-School Agreements.

There have been some updates to keep in line with the updated version of 'Keeping Children Safe in Education' in 2025, published by The Department for Education.

Key People

Designated Safeguarding Lead (DSL) / Team:	C. Stock
Online Safety Lead (if different):	C. Stock and A. Begum
Online Safety / Safeguarding Link governor:	Cllr Mrs J. Jones
RSHE / PSHE Lead(s):	C. Stock
Computing Subject Lead:	A. Begum
Network Manager / Technical Support:	Elementary ICT
Data Protection Officer:	Craig Stillwell

Contents

Overview:

- Purpose of the Policy
- Scope of the Policy
- Risks

Roles and Responsibilities:

- Headteacher
- Designated Safeguarding Lead
- Online Safety Lead
- Governors / Online Safety Governor
- All Staff (including Teaching and Support Staff)
- RSHE / PSHE Subject Leader(s)
- Computing Subject Leader
- Network Manager / Technical staff / Computing Subject Leader
- Data Protection Officer
- Children
- Parents / Carers
- Volunteers, Contractors (including Tutors) and Community Users

Education and Training:

- Children
- Staff and Governors
- Parents / Carers
- Wider Community

Technical Management:

- Infrastructure, Equipment, Security, Filtering and Monitoring
- Password Policy
- Mobile Technology (including BYOD)
- Use of generative AI
- Use of Digital and Video Images
- Communications
- Social Media – Staff (Protecting Professional Identity)
- Social Media – Children

Incident Management:

- Responding to Incidents

Appendices:

- Appendix 1: Communication Technologies
- Appendix 2: Dealing with unsuitable / inappropriate activities
 - 2.1: Usage restrictions form
 - 2.2: Actions and sanctions form – Child incidents
 - 2.3: Actions and sanctions form – Staff incidents
- Appendix 3: Sharing nudes and semi-nudes

Overview

Online safety is an integral part of safeguarding and requires a whole-school approach. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

“Governing bodies and proprietors must ensure that online safety is a continuing and integrated theme within the school's overall approach to safeguarding. This includes ensuring that online safety is clearly reflected across all relevant policies and procedures, is embedded within curriculum planning, and is incorporated into the training and ongoing professional development of all staff. Governing bodies must also ensure that the Designated Safeguarding Lead (and any deputies) have clear responsibilities for online safety, including oversight of the school's filtering and monitoring arrangements, and that parents and carers are effectively engaged and supported to promote safe online behaviour at home.”

(Aligned with Keeping Children Safe in Education (KCSIE) 2025)

Purpose of the Policy

Schools must have an online safety policy covering the safe use of internet and electronic communications technologies such as mobile phones and internet connected devices. The policy will highlight the need to educate children, young people and their families about both the benefits and risks of using technologies both in and away from the school context. It will also provide safeguards and rules to guide staff, children and visitors in their online experiences.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. There are additional duties under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. Revised “Keeping Children Safe in Education” guidance obliges schools and colleges in England to ‘ensure appropriate filters and appropriate monitoring systems are in place.’

Scope of the Policy

This policy applies to all members of the school community (including staff, children, volunteers, parents / carer, visitors, community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

The policy will be communicated to staff/children/community in the following ways:

- Policy to be available via the school office and website (and on the school network for staff)
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and children at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

- The school will monitor the impact of the policy using:
- Logs of reported incidents (logged in behaviour records and CPOMS)
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for networks activity
- Surveys / questionnaires of children, parents / carers and staff

All incidents will be reported to Governors termly via the Headteacher's report.

Risks:

The Department for Education's Keeping Children Safe in Education guidance recognises that online safety covers a wide and constantly evolving range of issues. These can broadly be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful material, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, and other content generated by AI or emerging technologies.
- **Contact:** being subjected to harmful online interactions with other users, including peer-to-peer pressure, commercial advertising, and adults posing as children or young people to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm, for example making, sending, and receiving explicit images (including consensual and non-consensual sharing of nudes or semi-nudes), sharing other explicit images, online bullying, or harmful interactions via social media and messaging platforms.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing, scams, or other financial exploitation.

Schools must also consider emerging online risks, including AI-generated content (such as deepfakes and misinformation), online radicalisation, and other new technologies that may impact the safety and wellbeing of children.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school (in some cases the roles described may be combined).

Headteacher

- To foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- To take overall responsibility for the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- To oversee and support the work of the Designated Safeguarding Lead (DSL) team, ensuring effective collaboration with technical staff to complete regular online safety audits in line with KCSIE requirements.
- To undertake training in both offline and online safeguarding in accordance with statutory guidance and Local Safeguarding Children Partnership expectations.
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- To ensure all staff undergo safeguarding training (including online safety) at induction and with regular updates, and that they agree to and adhere to all relevant policies and procedures.

- To ensure all governors and trustees undertake safeguarding and child protection training (including online safety) with regular updates, enabling them to provide strategic challenge and oversight.
- To take overall responsibility for data management and information security ensuring the school follows best practice in information handling.
- To work closely with the DPO, DSL and governors to ensure data protection processes support safe, legal and appropriate sharing of information, particularly where this relates to child protection.
- To ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, and protected email systems.
- To ensure all school technology, including remote learning systems, is selected and implemented using child-safety-first principles.
- To regularly review and drive the rationale behind filtering and monitoring decisions (in line with DfE standards), understanding what is blocked or allowed, for whom, when, and why.
- To understand and make all staff aware of procedures to be followed in the event of a serious online safety incident.
- To liaise regularly with the DSL on all online safety concerns and ensure they receive ongoing updates relating to school issues, local concerns and national guidance.
- To support safeguarding and technical staff in reviewing home-learning protections, remote-learning rules and digital safeguarding practices.
- To ensure suitable risk assessments are undertaken so the curriculum meets the needs of children, including the risk of children being radicalised.
- To ensure the school website meets statutory requirements.
- To report online safety incidents to Governors termly via the Headteacher's report.
- To ensure governors receive regular updates on the effectiveness of the school's online safety arrangements.

Designated Safeguarding Lead

- Take lead responsibility for online safety:
 - "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and for understanding the filtering and monitoring systems and processes in place). While the DSL may delegate some activities to appropriately trained deputies, the ultimate responsibility for safeguarding, including online safety, must remain with the DSL and cannot be delegated." (KCSIE 2025).
 - Ensure the school maintains an effective whole-school approach to online safety in line with KCSIE 2025.
 - Ensure the school complies with the DfE standards for filtering and monitoring and maintains oversight of how systems operate and are reviewed.
- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
 - sharing of personal data
 - access to illegal / inappropriate materials
 - inappropriate online contact with adults / strangers
 - potential or actual incidents of grooming
 - online bullying
 - additional risks learners with SEND face online
 - filtering and monitoring on school devices and school networks
 - emerging AI-related risks such as deepfakes, synthetic media, misinformation and harmful algorithmic content

NB it is important to emphasise that these are safeguarding issues, not technical issues; the technology simply provides a mechanism for safeguarding issues to develop.

- Facilitate training and advice for all staff on Keeping Children Safe in Education (2025), including sections covering online safety.
 - Ensure all staff (including supply staff) complete safeguarding and online-safety training at induction, including filtering and monitoring responsibilities, and receive regular updates.
 - Ensure all staff read the correct parts of KCSIE (Part 1 or Annex A, plus Annex B for those working directly with children).
 - Cascade knowledge of new online risks, behaviours and technologies throughout the school.
- To “liaise with staff (especially teachers, pastoral support staff, IT technicians, the mental health lead and SENCOs) on matters of safety, safeguarding and welfare, including online and digital safety, and when making decisions about referrals to external agencies.” (KCSIE 2025)
- Where the online safety lead is not the named or deputy designated safeguarding lead (DSL), ensure there is regular review and open communication between these roles and that the DSL’s overarching responsibility for online safety is not compromised.
 - Ensure curriculum areas (e.g., Computing, RSHE) delivering online-safety content do not contradict or dilute safeguarding expectations.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious concerns to arise online.
 - Use appropriate, non-victim-blaming language when managing concerns or recording incidents.
- Remind staff of safeguarding considerations during any review of remote-learning procedures and ensure the same standards of safety apply when children learn from home.
- Work closely with SLT, staff and technical colleagues to complete regular online-safety audits, including reviewing the technology in use within the school.
- Work with the Headteacher, DPO and governors to ensure a compliant data-management framework that enables safe, legal and appropriate information sharing, always prioritising child protection.
- Stay up to date with the latest online-safeguarding trends and undertake Prevent awareness training in line with KCSIE 2025 requirements.
- Review and update the Online Safety Policy, Acceptable Use Policies and all other related safeguarding documentation, ensuring consistency with behaviour, safeguarding, Prevent and pastoral policies.
- Ensure online-safety education is embedded across the curriculum and wider school life, in line with statutory RSHE requirements and the UKCIS Education for a Connected World framework.
- Promote online-safety awareness across the entire school community, including targeted support for parents and carers who may be harder to reach.
- Ensure all staff understand the procedures to be followed in the event of an online-safety incident, and that all incidents are logged and processed in line with safeguarding procedures.
- Ensure children and staff have secure ways to disclose concerns while off-site, including during isolation or remote learning periods.
- Ensure staff adopt a zero-tolerance, whole-school approach to all forms of child-on-child abuse, including those occurring online or through digital means.
- Pay particular attention to safeguarding in relation to online tutors, whether commissioned by the school or hired privately by parents, ensuring that appropriate expectations and safety information are provided.

Online Safety Lead

- To ensure “an effective whole-school approach to online safety that empowers the school to protect and educate children and staff in their use of technology, and establishes mechanisms

to identify, intervene in and escalate any concerns where appropriate.” (KCSIE 2025, para 138–142)

- To take day-to-day responsibility for online safety issues and to be alert to the potential for serious child protection concerns arising from online activity.
- To have a leading role in establishing, maintaining and regularly reviewing the school’s Online Safety Policy and related documents (e.g., Acceptable Use Policies, filtering & monitoring protocols).
- To promote awareness and commitment to online safety across the whole school community — including engaging parents and carers, especially those who may be harder to reach.
- To ensure that online safety education is embedded across the curriculum in line with statutory guidance (e.g., RSHE) and reinforced throughout wider school life and activities.
- To ensure that all staff are aware of the procedures that must be followed in the event of an online safety incident, and that all such incidents are recorded, logged and managed in the same way as other safeguarding concerns (e.g., via CPOMS).
- To ensure that the log of online-safety incidents is used to inform future developments in the school’s online-safety strategy and practice.
- To stay up to date with changing online-safety issues and relevant legislation or statutory guidance — including national developments in filtering/monitoring standards, cyber-security and emerging risks (e.g., AI, misinformation).
- To coordinate and facilitate online-safety training and guidance for all staff, either as part of wider safeguarding training or as additional, dedicated sessions.
- To communicate regularly with senior leadership (SLT) and the designated online-safety governor/committee — discussing current issues, reviewing anonymised incident logs, examining filtering and “change control” logs, and ensuring transparency of safeguarding practices.
- To oversee and discuss the school’s filtering and monitoring arrangements on all school systems with technical teams, governors, and staff — ensuring that while harmful content is blocked, the school avoids over-blocking that would unreasonably restrict legitimate teaching or learning. (As required under the DfE Filtering & Monitoring Standards and KCSIE 2025)
- To work with the Headteacher and technical teams to review and strengthen protections for children engaged in home learning or remote education — ensuring remote systems, platforms and procedures comply with online-safety principles.
- To regularly monitor the use of school technology and online platforms, ensuring that any misuse (or attempted misuse) is identified, reported, and managed in line with the school’s safeguarding policies.

Governors / Online Safety Governor

- To ensure that the school has in place policies and practices to keep children and staff safe online.
- To approve the Online Safety Policy and the wider online-safety strategy, and review its effectiveness.
- To ensure all staff undergo safeguarding and child protection training (including online safety and reminders about filtering and monitoring, in line with DfE standards).
- To undergo (and encourage all governors/trustees to undergo) safeguarding and child protection training — including online safety — at induction, and ensure this is regularly updated.
- To support the school in encouraging parents and the wider community to become engaged in online safety activities.
- To ask how the school has reviewed protections for children in the home and remote-learning procedures, rules and safeguards.
- To ensure the school has appropriate filtering and monitoring systems in place, that these are regularly reviewed for effectiveness, and that leaders understand their responsibilities under the DfE Filtering & Monitoring Standards.

- To ensure that the leadership team and relevant staff have an awareness and understanding of the filtering and monitoring systems, manage them effectively, and know how to escalate concerns.
- To appoint (or act as) a named Filtering and Monitoring Governor to work closely with the DSL and technical colleagues on the school's filtering and monitoring standards.
- To check that all school staff have read KCSIE Part 1, and that SLT and all staff working directly with children have read Annex B.
- To ensure that children are taught about safeguarding — including online safety — as part of a broad and balanced curriculum, and to support a whole-school approach to online safety with a clear policy on mobile technology.
- The role of the Online Safety Governor may include:
 - regular strategic reviews with the Online Safety Lead / DSL
 - regular monitoring of online safety incident logs (CPOMS)
 - regular monitoring of filtering / change-control logs (Impero Alert)
 - reporting to the relevant Governing Body committees

The Governor role may be combined with that of the Child Protection / Safeguarding Governor

All Staff (including Teaching and Support Staff)

- To ensure they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices (including safeguarding provisions for home learning and remote teaching) and have read relevant sections of KCSIE 2025.
- To understand that online safety is a core part of safeguarding; as such it is everyone's responsibility.
- To read, understand, sign and adhere to the school Online Safety Policy and staff Acceptable Use Agreement, alongside the school's main Safeguarding and Child Protection Policy, the Staff Code of Conduct/Handbook, and relevant parts of KCSIE, in order to support a whole-school safeguarding approach.
- To record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- To report any online safety concern, no matter how small, to the Designated Safeguarding Lead (as named in the AUP).
- To ensure that any digital communications with children / parents / carers should be on a professional level and only through school-based systems, e.g., not on personal email, mobile phones, etc.
- To embed online safety in all aspects of school life, both across the curriculum and outside the classroom.
- Curriculum subject leaders to identify opportunities to thread online safety through their curriculum subject and work with class teachers to implement.
- To ensure that children understand and follow the Online Safety Policy and Child Acceptable Use Agreement.
- To supervise and guide children carefully when engaged in learning activities involving online technology (including extra-curricular, extended school activities and home learning where relevant).
- When supporting children remotely, be mindful of additional safeguarding considerations.
- To ensure that children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To prepare and check online source and resources before using within the classroom.
- To monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- To model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and on social media; in all aspects upholding the reputation of the school and the profession.
- To be aware of security best-practice, including password safety and phishing strategies.

- To understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- To maintain awareness of current online safety issues and risks (including those highlighted in the 2025 KCSIE and the start of this policy), and to avoid using language that is scaring or victim-blaming when addressing online safety with children.
- To be aware of the DfE standards for filtering and monitoring and provide feedback to the DSL regarding over blocking, gaps in filtering/monitoring, or attempts by children to bypass protections.
- To take responsibility for the physical monitoring of children' online devices during any session or class they are supervising.

RSHE / PSHE Subject Leader

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the RSHE / PSHE curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their children' lives.
- RSHE policy must be published on the school website, in line with statutory requirements.

Computing Subject Leader

- To oversee the delivery of the online safety element of the Computing curriculum, ensuring progression in the content to reflect the different and escalating risks that children face and in accordance with the national curriculum.
- Work closely with the DSL and online safety lead to ensure a shared understanding of the issues, approaches and messages for the computing curriculum.
- Work closely with the RSHE / PSHE lead(s) to avoid overlap and ensure a complementary whole-school approach to online safety.
- Work closely with the DSL and all other relevant staff to ensure consistency and clarity in the messaging, teaching approaches and safeguarding responses within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common, safe and consistent approach, in line with acceptable-use agreements and the school's filtering and monitoring arrangements.
- To work with the headteacher to ensure the school website meets statutory DfE requirements.
- Embed awareness of risks from emerging online harms, including:
 - self-generative artificial intelligence
 - financial extortion and online scams
 - sharing intimate images and online coercion

These themes should be incorporated sensitively and appropriately in line with statutory guidance.

- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools, supporting children to navigate the online world safely and confidently regardless of device, platform or app.
- Work collaboratively with all other curriculum leads to ensure online safety themes are consistent across the curriculum and reflect a whole-school safeguarding approach.

Network Manager (Elementary ICT)

- To manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, and with adequate protection, encryption and backup for data, including disaster recovery plans and auditable access controls.
- To report any online safety related issues that come to their attention in line with school policy.

- To work closely with the DSL / online safety lead / data protection officer / RSHE lead to ensure that school systems and networks reflect school policy and that there are no conflicts between educational messages and practice.
- To support the headteacher and DSL team as they review protections for children in the home and remote-learning procedures, rules and safeguards.
- To support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and SLT, ensuring systems work on new devices and services before release.
- To ensure the school's policy on web filtering is applied and updated on a regular basis, carrying out regular reviews and annual checks in line with KCSIE and DfE standards.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up to date with the school's online safety policy, technical information and legislation in order to effectively carry out their online safety role, and to inform and update others as relevant.
- To maintain up-to-date documentation of the school's online security, technical procedures and monitoring arrangements.
- To collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology, including annual online safety audits.
- To support safeguarding teams to understand and manage filtering and monitoring systems, including reviewing what is blocked or allowed, and ensuring over-blocking does not create unreasonable restrictions.
- To monitor the use of school technology, online platforms and social media presence and ensure any misuse or attempted misuse is identified and reported in line with school policy.
- To work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer

Further information regarding the Data Protection Officer (DPO) and General Data Protection Regulation (GDPR) can be found in the Data Protection / GDPR policy.

- To oversee the data protection strategy in school, and ensure compliance with GDPR legislation.
- To ensure best practice in information management, i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- To ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.
- To provide data protection expertise, training, and guidance to staff, supporting compliance with data protection and safeguarding policies, and ensuring policies are aligned with each other and with this Online Safety Policy.
- To recognise that data protection legislation does not prevent the sharing of information for safeguarding purposes. As stated in KCSIE 2025, "The UK GDPR and Data Protection Act 2018 do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of safeguarding and promoting the welfare and safety of children."

Children

- To read, understand, sign, and adhere to the Child Acceptable Use Policy (AUP) annually.
- To understand the importance of reporting abuse, misuse, or access to inappropriate materials, including any concerns about a member of school staff, supply teacher, or visitor.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology, whether at school, at home, or elsewhere.
- To understand the importance of adopting safe behaviours and good online safety practices when using digital technologies out of school, including on social media; the school's Online Safety Policy applies to their actions outside school.

- To treat home learning during any isolation, quarantine, or school closure in the same way as regular learning in school, behaving as if a teacher or parent were supervising.
- To avoid private communications or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
- To develop good research skills and understand the need to avoid plagiarism and uphold copyright regulations.
- To know, understand, and adhere to the school policy on the use of mobile devices and digital cameras, including taking or using images and preventing online bullying.
- To understand the benefits, opportunities, risks, and dangers of the online world, and know who to talk to at school or outside school if problems arise.

Parents / Carers

- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement, including the use of photographs and video images and children's use of the internet.
- To inform the school of any changes in consent to the use of photographs and video images.
- To read, understand and promote the school Child Acceptable Use Agreement with their children and encourage their children to follow it.
- To consult with the school if they have any concerns about their children's use of technology.
- To model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media.
- Encourage children to engage fully in home-learning.

Volunteers, Contractors (including Tutors and Supply Staff) and Community Users

- To read, understand, sign and adhere to an acceptable use policy.
- To support the school in promoting online safety.
- To maintain an awareness of current online safety issues and guidance.
- To model safe, responsible and positive behaviours in their own use of technology.
- To report any concerns to the DSL / online safety lead.

Education and Training

Children

"Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online." Keeping Children Safe in Education, para 129 DfE 2025

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children 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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety message across the curriculum. The following subjects have the clearest online safety links:

- Relationships Education (Primary), Relationships and Sex Education (Secondary) and Health Education (all); also known as RSHE
- Computing
- Citizenship

In planning their online safety curriculum, schools are also advised to refer to:

- DfE Teaching Online Safety in Schools guidance (2019)

- Education for a Connected World framework (UK Council for Internet Safety, 2020)

Additional links, Keeping Children Safe in Education 2025 para 133.

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of RSHE / PSHE / Computing / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Children should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information (critical thinking, 'fake news')
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making (NB additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet).
- Children should be helped to understand the need for the child Acceptable Use Agreement, sign and follow the guidance outlined in the agreement.
- Children should be taught and encouraged to adopt safe and responsible use of technology both within and outside school, including appropriate online behaviour and keeping personal information private.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what children/children are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation, and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.
- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Staff and Governors

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Governors are invited to online safety training events.

Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- An audit of the online safety training needs of all staff will be carried out regularly.
- The Online Safety Lead will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy will be presented to and discussed by staff in staff meetings.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Displays in school / at parents' evenings
- Parent / carer online safety workshop
- Reference to the relevant websites / publications for further support

Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experiences. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.

Technical Management

Infrastructure, Equipment, Security and Filtering

The school, with the support of Elementary ICT, is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible, and that the policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their online safety responsibilities.

- There will be regular reviews and audits of the safety and security of the school technical systems.
- The school network has user-defined policies ensuring secure documents are only accessible by specific users.
- The school has educational, filtered, secure broadband connectivity.
- Internet access is filtered for all users to keep users safe, including from terrorist and extremist material. Illegal content is filtered by the broadband provider, and only nominated staff are able to make a change to the filtering system.
- The school will ensure, to the best of their ability, that the filtering system prevents children using websites designed to bypass the filtering.
- The school has a secure wireless network to ensure access is restricted to school devices
- If staff or children come across unsuitable on-line materials, the site is reported to the appropriate person(s) in line with school policy.
- The school checks their virus protection is updating regularly and informs their IT Support Service provider of any issues.
- Staff and children have access to the school network via a login suitable to their 'role'. Staff do not share their login details.
- Staff access to the management information system is controlled through a separate password for data security purposes. Staff only have access to the modules they require for their role, and passwords are not shared.
- The school checks that their data is backed up, and that data can be retrieved.

- The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Guest accounts are only used for a short period of time by temporary staff.
- Guest access to Wi-Fi is only accessible with a guest password.
- The school requires all users to log off when they have finished working, and to log off (or lock if not a shared computer) when leaving the computer unattended.
- The school ensures that all child level or personal data sent over the internet is encrypted or sent using an approved system, for example DfE S2S, encrypted / secure email.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Children use a child-friendly internet search engine.
- At our school we recognise that generative AI sites can pose data risks so staff are not allowed to enter child data and where they use them, they must be approved. For children and young people, we block the generative AI category and only allow specific sites for adults. These are [ChatGPT]; we know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines.

Password Policy

- The school makes it clear that staff and children must always keep their passwords private and not share them with others.
- If a password is compromised the school should be notified immediately.
- Staff are required to use strong passwords for network / email / MIS.
- Staff are required to change their MIS passwords at least twice a year.
- Staff with administrator rights are required to change their email and computer passwords at least twice a year.

Mobile Technology

- Personal devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Staff should not use their personal device when contacting children or parents; there should be access to a school phone.
- The school does not allow children below year 5 to bring in phones and advises that children's mobile phones should not be brought into school. However, if year 5 and 6 children do bring in phones, they are asked to hand them in to the office for safe keeping.
- Staff who work directly with/ supervise children should leave their mobile phones on silent and not use them in the presence of children unless as part of an approved and directed curriculum-based activity.
- The recording, taking and sharing of images, video and audio on any personal device is to be avoided, except where it has been explicitly agreed otherwise by the headteacher in line with KCSIE 2025 and the Statutory Framework for EYFS.
- The school reserves the right to search the content of any mobile or handheld device on school premises where there is a reasonable suspicion that it may contain undesirable material.

Use of generative AI

At Becontree Primary School, we acknowledge that generative AI platforms (e.g., ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with children, staff and parents – their practical use as well as their ethical pros and cons.

- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some children – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots).

Staff use of generative AI for marking and planning

Becontree Primary School currently allows staff to use approved generative AI tools (e.g., ChatGPT) to support planning, resource creation and, where appropriate, aspects of marking such as generating success criteria, feedback statements, or exemplar responses.

- Staff must not input any personal data about children, parents or staff into AI platforms.
- AI-generated text must be reviewed, edited and validated by the teacher to ensure accuracy, appropriateness, and alignment with school policy and curriculum intent.
- All staff to receive training on safe, ethical and effective use of generative AI, and ongoing support is provided through INSET sessions and school digital-lead support.

Child access to generative AI

At present, children do not have access to any generative AI platforms (including text-, image-, video- or audio-generation tools). This is due to age restrictions, safeguarding considerations, and the difficulty in effectively filtering and monitoring such platforms. The school will continue to take a risk-based approach, reviewing this position as technology, guidance and curriculum needs evolve.

Approval process for new AI platforms

In line with KCSIE 2025, Becontree Primary School has a clear process for approving any new digital platform, app or generative AI tool before it is used by staff.

- New AI platforms or tools may only be used in school if they meet safeguarding, data protection and curriculum standards.
- All requests for new platforms must be submitted to the Headteacher for approval.
- As part of this process, the Designated Safeguarding Lead (DSL) will lead on assessing safeguarding and online-safety risks, including considerations of data protection, age-appropriateness and potential safeguarding concerns, in line with KCSIE.
- Each platform will undergo a full risk and suitability assessment carried out in consultation with Elementary ICT, including checks on technical security, filtering and monitoring implications, and overall educational value.
- The Senior Leadership Team (SLT) will ensure that any approved platform aligns with the school's wider safeguarding, curriculum and operational requirements.
- The Governing Body maintains strategic oversight and will review the effectiveness of the school's approval process as part of its wider safeguarding responsibilities.
- Only platforms authorised through this process will be permitted for staff use.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website / social media / local press.
- Digital media should be used in accordance with the home school agreement.
- Children' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website will be selected carefully and will comply with good practice guidance on the use of such images.
- Child's work can only be published with the permission of the child and parents or carers.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Schools need to consider the benefit of using these technologies for education whilst reducing their risks (see **appendix 1**).

- The school email service may be regarded as safe and secure and is monitored. Staff and children should only use the school email service to communicate with others when in school, or on school systems.
- Any digital communication between staff and children or parents / carers must be professional in tone and content, and must only take place on school approved systems. Personal email addresses or social media must not be used for these communications.
- Users must immediately tell an appropriate member of staff if they receive any communication which is offensive, discriminatory, threatening or bullying in nature, and should not respond to any such communication.
- Staff or child personal contact information should not be published. The contact details given online should be the school office.
- Children should be taught about online safety issues such as the risks attached to the sharing or personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Children need to be educated in how to deal with incoming email and associated attachments.
- The school should consider how e-mail from children to external bodies is presented and controlled.
- Whole class / group email addresses may be used at KS1, while children / children at KS2 and above will be provided with individual school email addresses for educational use.

Social Media – Staff (Protecting Professional Identity)

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of children, the school and the individual when publishing material online. Expectations for teachers' professional conduct are set out in Teachers Standards

2012. Ofsted's online safety inspection framework reviews how a school protects and educates staff and children in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools have a duty of care to provide a safe learning environment for children and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

- The school has clear reporting guidance, including responsibilities, procedures and sanctions.
- The school ensures that personal information is not published.
- All school staff sign the Acceptable Use Agreement indicating they understand and will follow the guidance contained.
- School staff ensure they make no reference in social media to children, parents / carers or school staff.
- School staff should not engage in online discussion on personal matters relating to members of the school community.
- School staff should ensure that personal opinions are not attributed to the school or local authority.
- School staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Becontree Primary School does not currently have any social media accounts. However, if official school social media accounts are established there should be:

- A process for approval by senior leaders.
- A social media risk assessment carried out.
- A social media policy in place.
- Clear processes for the administration and monitoring of these accounts.
- A code of behaviour for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.

Personal use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Social Media – Children

- The school will control access to social networking sites, and where relevant educate children in their safe use.
- Children will be advised never to give out personal details of any kind which may identify them, their friends or their location and to use nicknames and avatars when using social networking sites.

- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged children.

Incident Management

Responding to Incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE / RSHE and Citizenship). General concerns must be handled in the same way as other safeguarding concerns.

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Computing Policy
- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour and Attitudes Strategy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- GDPR Policies

All online safety incidents are logged either in the school's class behaviour files or in CPOMS, as appropriate.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible, or very rarely, through deliberate misuse. This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

See **appendix 2** for *Dealing with Unsuitable / Inappropriate Activities, including school actions and sanctions pro-formas*, and **appendix 3** for *Sharing nudes and semi-nudes' advice*

Some internet activity, e.g., accessing child abuse images or distributing racist materials is illegal and would obviously be banned from school. Other activities e.g., cyberbullying would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context.

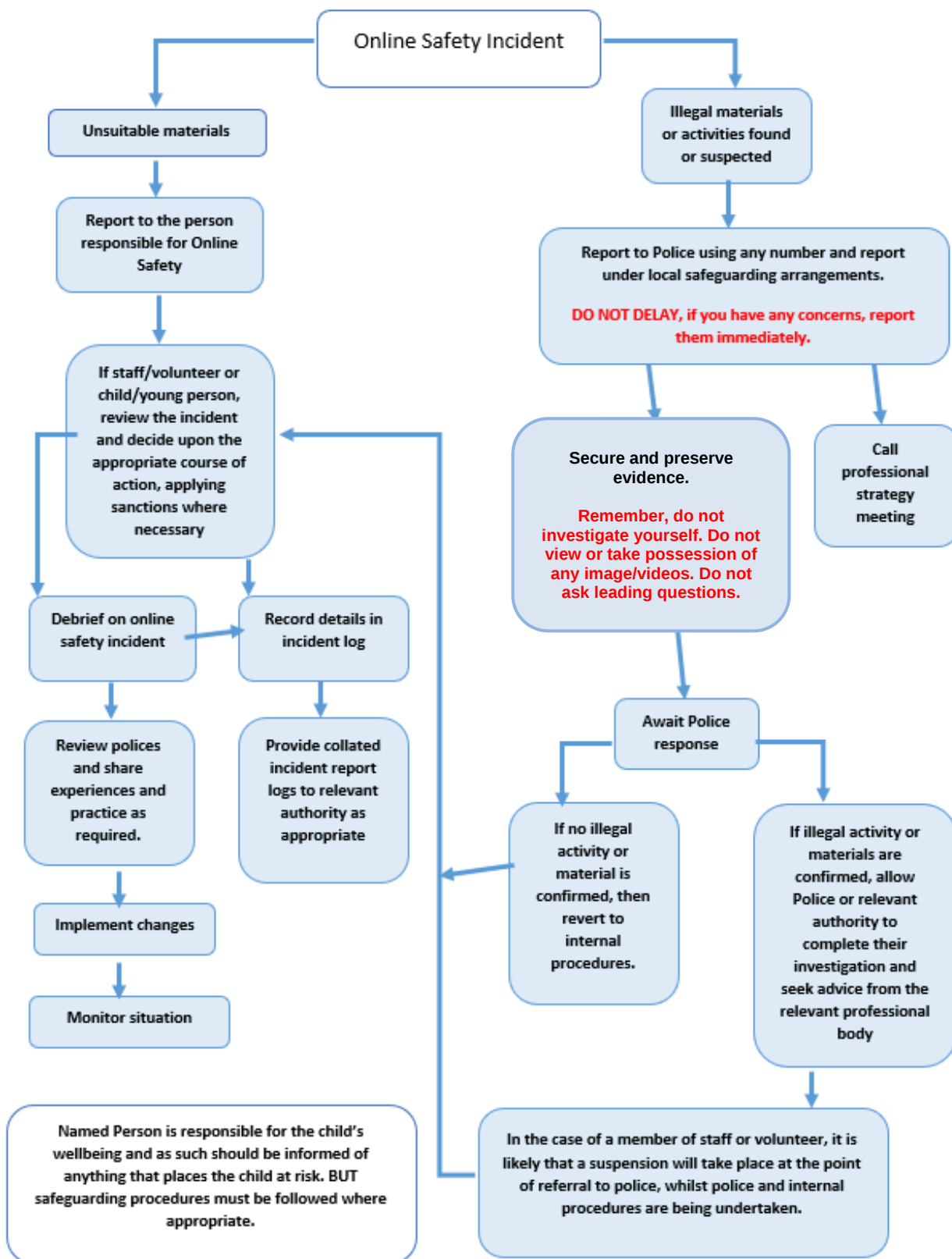
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures; actions and sanctions forms (**appendix 2.2 and 2.3**) show the responses have been agreed.

- If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the incident will be reported to the appropriate bodies immediately (see right hand side of **flowchart** below).

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - offences under the Computer Misuse Act (see User Actions chart above)
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.



Appendix 1

Communication Technologies

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

Communication Technologies	Staff & other adults				Children / Children			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with permission	Not allowed
Mobile phones may be brought to the school (Children – non smartphones only)	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking of photos on mobile phones / personal cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices		X					X	
Use of personal email addresses for work/school purposes				X				X
Use of school email for personal emails				X				X
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs		X					X	

Appendix 2

Dealing with unsuitable / inappropriate activities

2.1 – Usage restrictions form

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of school when using school equipment or systems. The school policy restricts usage as follows.

Usage restrictions		Acceptable	Acceptable at certain times *	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children					X
	Possession of an extreme pornographic image					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation)					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school, or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, website or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			X			
Online gaming (non-educational)					X	
Online gambling					X	
Online shopping / commerce				X		
File sharing		X				
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. YouTube		X				

* usually with prior permission and monitored

2.2 – Actions and sanctions form: Child incidents

Actions and Sanctions: Child Incidents Repeated incidents of any of the below will be referred to SLT	Refer to class teacher / tutor	Refer to LMT / Phase Leader	Refer to Headteacher / SLT	Refer to Police	Refer to technical support staff for action e.g., filtering / security etc.	Inform parents / carers	Appropriate sanction in line with behaviour and attitudes strategy. E.g. Warning, removal of network / internet access rights
Deliberately accessing or trying to access material that could be considered illegal (see previous list)			X	X		X	X
Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X		X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X		X	X	X
Unauthorised downloading or uploading of files	X	X	X		X	X	X
Allowing others to access school network by sharing username and passwords			X			X	X
Attempting to access or accessing the school network using another child's account			X			X	X
Attempting to access or accessing the school network using the account of a member of staff			X			X	X
Corrupting or destroying the data of other users			X			X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X	X
Actions which would bring the school into disrepute or breach the integrity of the ethos of the school			X			X	X
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X	X
Deliberately accessing or trying to access offensive or pornographic material			X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X	X	X
Continued infringements of any the above, following previous warnings or sanctions			X			X	X

2.3 – Actions and sanctions form: Staff incidents

Actions and Sanctions: Staff Incidents	Refer to Headteacher / SLT	Refer to Local Authority / HR / Governors / DPO / LADO	Refer to Police	Refer to technical support staff for action re filtering etc.	Disciplinary action e.g. warning, suspension etc. following school procedure, with the ability to skip
Deliberately accessing or trying to access material that could be considered illegal (see previous list)	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X				X
Unauthorised downloading or uploading of files	X				X
Allowing others to access school network by sharing username and passwords, or attempting to access or accessing school network using another person's account	X			X	X
Careless use of personal data, e.g. holding or transferring data in an insecure manner	X				X
Deliberate actions to breach data protection or network security rules	X	X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with children	X	X	X		X
Actions which could compromise the staff member's professional standing	X	X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X
Using proxy sites or other means to subvert the school's filtering system	X			X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X
Breaching copyright or licencing regulations	X				X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X

We would seek advice from a relevant body for advice, for some actions

Appendix 3

Sharing nudes and semi-nudes

How to respond to an incident – an overview for education settings

From Department for Digital, Culture, Media & Sport and UK Council for Internet Safety

In the latest advice for schools and colleges (UKCIS, 2024), the sharing of nudes and semi-nudes is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year-olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

- **Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. Your setting's child protection policy should outline codes of practice to be followed.**
- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal.**
- If you have already viewed the imagery by accident (e.g., if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

For further information, download the full guidance from:

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people> (UKCIS, 2024)