

Charles Kingsley's CE Primary School

Online Safety Policy (including Acceptable Use)

1853 CHARLES KINGSLEY'S SCHOOL 2003



SCHOOL

CHURCH

COMMUNITY

**This policy was reviewed by the Governing Body:
Autumn Term 2026**

Next Review Date: Autumn Term 2027

This Online Safety Policy outlines the commitment of Charles Kingsley's CE School to safeguard members of our school community online in accordance with statutory guidance and best practice.

KCSIE 2026

162. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Charles Kingsley's CE 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.

Online Safety is an essential part of our safeguarding policies.

Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as:

- providing help and support to meet the needs of children as soon as problems emerge,
- protecting children from maltreatment, whether that is within or outside the home, including online,
- preventing the impairment of children's mental and physical health or development,
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care, and
- taking action to enable all children to have the best outcomes. (KCSIE 2026)

The above statutory guidance defines child protection as part of safeguarding and promoting welfare. Child protection is the activity undertaken to protect specific children who are suffering, or are likely to suffer, significant harm.

This involves safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.

Charles Kingsley's CE Primary School recognises that online safety is an integral part of safeguarding and child protection. Online safety is a running and interrelated theme that is reflected throughout safeguarding policies, behaviour expectations, curriculum planning, staff training, risk assessments and parental engagement.

The school adopts a whole-school approach that empowers children, staff and parents to use technology safely and responsibly while establishing effective procedures to identify, intervene and escalate concerns where appropriate.

The Governing Body and Staff at Charles Kingsley's CE Primary School believe that it is the right of every child to lead their lives in safety and to be protected from harm and in that respect we seek to safeguard and promote the welfare of all our pupil whilst complying with the guidance issued by the local safeguarding Board and the Department for education.

Charles Kingsley's CE Primary School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of the Governing body and staff recognises that safeguarding against

radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.

We believe that the welfare and safety of every child **MUST** be our primary concern.

Policy and leadership

Responsibilities

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

Headteacher and Assistant heads (also DSL and DDSLs)

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and assistant heads should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff .
- The headteacher and assistant heads are responsible for ensuring that the Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher and assistant heads will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher and assistant heads will receive regular monitoring reports from the Online Safety Lead.
- The headteacher assistant heads will work with the responsible Governor (Angela Bidgood), and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance “Keeping Children Safe in Education” **2026** states:

“156. Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities (SEND).

161. Whilst it is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place, they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

164. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.”

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document “Online Safety in Schools and Colleges – questions from the Governing Body”.

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

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors group/meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- ensure the school meets the Department for Education Cyber Security Standards for Schools and Colleges.
- receive assurance that cyber security risks are appropriately managed.
- ensure online safety and cyber security are considered within wider safeguarding and risk management arrangements.

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

Designated Safety Lead (DSL) – Hannah Popplewell (head teacher)

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”

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- understand the filtering and monitoring systems used by the school and how safeguarding concerns are identified, managed and escalated.

- work alongside the IT Provider and Senior Leadership Team to review filtering and monitoring arrangements at least annually.
- understand the safeguarding implications of emerging technologies, including Artificial Intelligence (AI) and Generative AI.
- ensure that online safety remains a key safeguarding priority across the curriculum and wider school life.

Online Safety Lead (also Computing Lead)

The Online Safety Lead will:

- work closely with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with class teachers to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - o content
 - o contact
 - o conduct
 - o commerce

This includes ensuring that generative AI is not available for children to use in school.

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete Purple Mash program
- RSHE and SRE program
- A mapped cross-curricular program
- assemblies and pastoral program
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- understand the four categories of online risk (Content, Contact, Conduct and Commerce) and recognise how these may affect children.
- understand the safeguarding risks associated with Artificial Intelligence, including deepfakes, AI-generated content and AI-enabled online grooming.
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements)
- they immediately report any suspected misuse or problem to DSL through My concern for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated. That they don't promote the use of generative AI with the children and is not available for children to use in school.

IT Provider (PSD)

The DfE Filtering and Monitoring Standards says:

“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”

“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”

“The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems*
- providing filtering and monitoring reports*
- completing actions following concerns or checks to systems”*

“The IT service provider should work with the senior leadership team and DSL to:

- procure systems*
- identify risk*
- carry out reviews*
- carry out checks”*

“We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision.”

The IT Provider (PSD) is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy

- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

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

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.

Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to

avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.

- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.
- Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

Policy

Online Safety Policy

The DfE guidance “Keeping Children Safe in Education” states:

“Online safety and the school or college’s approach to it should be reflected in the child protection policy”

The school Online Safety Policy:

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

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school’s expectations on the responsible use of technology by its users. It is acknowledged by staff as part of their conditions of employment. Parents and carers are asked to acknowledge the agreement when their child joins the school either in Year R or as part of the induction pack. These agreements may be discussed and promoted throughout the year. The range of acceptable use agreements are in the appendices.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated through:

- Induction packs for new started
- staff induction
- yearly statutory reading and training
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

When using communication technologies, the Charles Kingsley's CE School considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

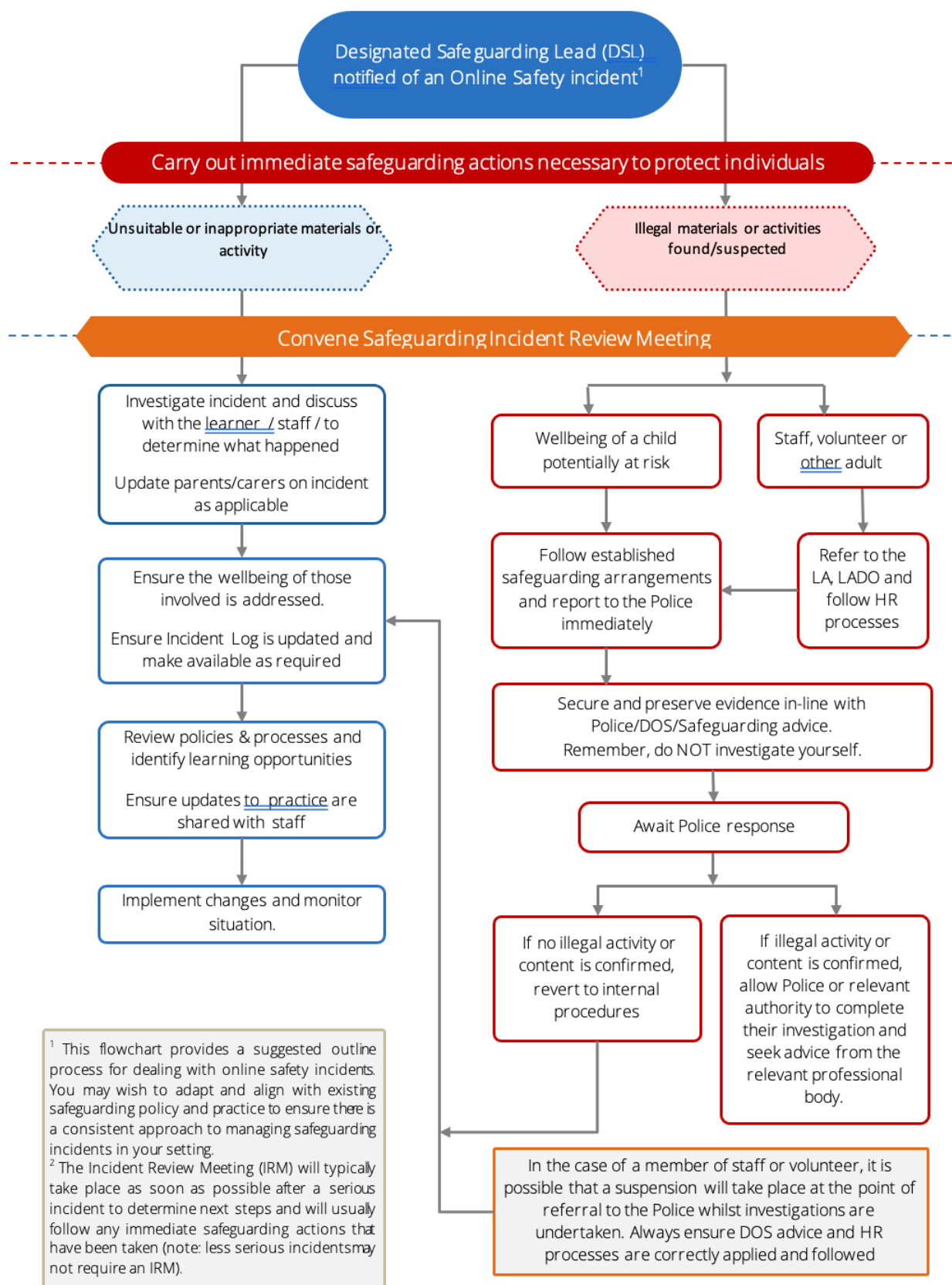
Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include: routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
 - o Non-consensual images
 - o Self-generated images
 - o Terrorism/extremism
 - o Hate crime/ Abuse
 - o Fraud and extortion
 - o Harassment/stalking
 - o Child Sexual Abuse Material (CSAM)
 - o Child Sexual Exploitation Grooming
 - o Extreme Pornography
 - o Sale of illegal materials/substances
 - o Cyber or hacking offences under the Computer Misuse Act
 - o Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the LADO (Low Level concerns policy, Whistleblowing policy)
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, the incident will be investigated using the flowchart available to staff to support the decision-making process for dealing with online safety incidents.



School actions

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.

The use of Artificial Intelligence (AI) systems at Charles Kingsley's CE School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

As a school will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- Charles Kingsley's CE School acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

(See A.I. Policy)

Mobile Phones

Charles Kingsley's CE Primary School supports the Department for Education expectation that schools should be mobile phone-free environments wherever possible.

Pupils should not access personal mobile phones during the school day unless exceptional circumstances have been agreed by the Headteacher.

Staff are expected to use personal mobile devices professionally and in accordance with the Staff Code of Conduct and Acceptable Use Policy.

Remote Education

Where remote education is provided, the school will ensure that safeguarding arrangements remain effective. Staff will only use approved school communication platforms and pupils will only access approved online learning environments. Parents will be informed of the platforms used and appropriate expectations for online learning.

Online Safety Curriculum

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the Charles Kingsley's CE School's online safety provision. Learners

need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The online safety curriculum is designed to be age-appropriate and responsive to emerging technologies and risks. It includes teaching pupils about:

- healthy and respectful online relationships;
- online consent and personal boundaries;
- recognising online abuse and exploitation;
- misinformation and disinformation;
- deepfakes and AI-generated content;
- online scams and phishing;
- pornography and inappropriate content;
- misogyny, discrimination and harmful online influences;
- reporting concerns and seeking trusted adult support;
- digital resilience, critical thinking and responsible use of technology.

Teaching is adapted to meet the needs of all learners, including those with Special Educational Needs and Disabilities (SEND) and other vulnerable groups.

The Online Safety Curriculum and the new RSHE requirements for online safety awareness and wellbeing online work together.

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for:

“a carefully sequenced RSHE curriculum, based on the Department for Education’s (DfE’s) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of ‘nudes’..”

Keeping Children Safe in Education 2026 states:

“164. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.”

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

- A planned online safety curriculum for all year groups matched against to a nationally agreed framework and is regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. RHSE; SRE; Literacy etc
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The Being safe in the Digital world programme is accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

- Learners 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 (including where the information is gained from Artificial Intelligence services)
- Learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit
- It is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through: (amend as relevant)

- mechanisms to canvass learner feedback and opinion.
- appointment of wellbeing ambassadors
- learners contribute to the online safety education programme e.g. peer education, older students leading lessons for younger learners, online safety campaigns
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Online Safety Training

Staff/volunteers

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

151. Governing bodies and proprietors should ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see paragraphs 171-175 for further information) at induction. The training should be regularly updated. Induction and training should be in line with any advice from local safeguarding partners.

152. In addition, all staff should receive regular safeguarding and child protection updates, including online safety (for example, via email, e-bulletins, staff meetings) as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

153. Governing bodies and proprietors should recognise the expertise staff build by undertaking safeguarding training, and from managing safeguarding concerns on a daily basis. Opportunity should therefore be provided for staff to contribute to and shape safeguarding arrangements and the child protection policy.

154. Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including in relation to online safety (paragraphs 162-166) and for children to be taught about safeguarding, including in relation to online safety (paragraphs 162-166), that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.”

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school’s annual safeguarding, data protection and cyber-security training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- Designated Safeguarding Lead will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding.

A higher level of training will be made available to the Online Safety (Safeguarding) Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school’s filtering and monitoring provision, in order that they can participate in the required checks and reviews.

Families

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 online 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 seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority/MAT

Adults and Agencies

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

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

Technology

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" 2026 states:

171. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and ensure that a review of their effectiveness is carried out at least once every academic year. Reviews should be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. They should include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record should be kept of these checks. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

172. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.

I 74. Schools can use the department's 'Plan technology for your school service' to self-assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them."

The DfE's 'Plan technology for your school service' will be used over the following year.

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility the filtering and monitoring provision. Filtering and monitoring processes are reviewed (at least annually) by the DSL, Online safety Lead and a governor with the involvement of the IT Service Provider.

The effectiveness of filtering and monitoring systems will be reviewed at least annually by:

- the Headteacher (DSL)
- IT Provider (PSD)
- Online Safety Governor

The review will include:

- testing filtering across all internet-enabled devices
- reviewing monitoring alerts
- checking blocked categories
- confirming appropriate safeguarding escalation routes
- recording outcomes and actions taken.

Filtering

The DfE Technical Standards for Schools and Colleges states:

"Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

- a member of the SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and IT support are clearly defined
- 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 and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures

- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines

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

Monitoring

The DfE Technical Standards for Schools and Colleges states:

“Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user’s activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.”

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance.

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users: (Schools may wish to provide more specific details of their monitoring systems)

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- 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 monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- Monitoring enables alerts to be matched to users and devices.
- Where AI –supported monitoring is used, the purpose and scope of this is clearly communicated

Technical Security

Charles Kingsley’s CP School’s technical systems are managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.

- All users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
 - All school networks, devices and system will be protected by secure passwords.
 - The administrator passwords for school systems are kept in a secure place, e.g. school safe.
 - There will be regular reviews and audits of the safety and security of school technical systems
 - Servers, wireless systems and cabling are securely located and physical access restricted
 - Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
 - There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
 - Sarah Turner is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
 - Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
 - Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
 - Staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
 - Removable media is not permitted unless approved by the SLT/IT service provider
 - Guest users are provided with appropriate access to school systems based on an identified risk profile.
 - Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- (See A.I. policy and Cyber-security policy)

Social media

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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

Charles Kingsley's CE School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.

- clear reporting guidance, including responsibilities, procedures, and sanctions.

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- 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
- the school permits reasonable and appropriate access to personal social media sites during school hours

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school will effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.

- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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 (as such use is not covered by the Data Protection Act). 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 learners 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, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Arbor generated emails

The school website is hosted by Primary Site. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation and is set out in the school Data Protection Policy.

Cyber Security

The DfE Cyber security standards for schools and colleges explains (updated June 2026):

“Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised*
- impact on student outcomes*
- a significant data breach*
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure*
- financial loss*
- reputational damage”*

The school recognises that cyber security forms part of safeguarding. Appropriate technical and organisational measures are implemented in line with the Department for Education Cyber Security Standards for Schools and Colleges to reduce the risk of disruption, data breaches and safeguarding incidents.

The staff and governors at Charles Kingsley’s CE School are discussing Cyber-security around our school and devise an action plan to ensure we have an accurate cybersecurity policy, processes and procedures. **A cyber-security policy has been drafted.**

We will consider the following statements, and amend them in the light of our current cybersecurity processes and procedures:

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (in partnership with their technology support partner), has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school’s governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school’s education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Outcomes

The impact of this Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

Review

The Online Safety Policy and associated risk assessment will be reviewed at least annually by the Governing Body.

This review will consider:

- emerging technologies;
- Artificial Intelligence developments;
- filtering and monitoring effectiveness;
- cyber security risks;
- safeguarding incidents;
- pupil voice;
- staff feedback;
- parental feedback;
- national guidance and local safeguarding priorities.

The school will use recognised self-review tools, such as the UKCIS Online Safety Audit or 360Safe, to support continuous improvement.

This document has used the SWGfL template as a basis of this policy.

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline

Appendices

Appendix A – Staff (and Volunteer) Acceptable Use and Online Safety Agreement

Appendix B – Pupil, Parent/Carer Acceptable Use Agreement

Appendix C - IT Resources and access updated yearly

Appendix A

Staff (and Volunteer) Acceptable Use and Online Safety Agreement

Charles Kingsley's C of E (VA) Primary School Policy

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This online safety policy is intended to ensure: that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policies, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using digital technologies and systems
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school
- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack

When using AI systems in my professional role I will use these responsibly and:

- will only use AI technologies approved by the school
- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
- to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
- will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being

When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment.

I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.

When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.

For security and safety:

- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities, within or outside of the school.

I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.

I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

I confirm that I have read and understood the Online Safety Policy and agree to abide by it. I understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of IT facilities, I can seek such clarification from the Online Safety Lead (Clare Price) or DSL.

The Acceptable Use Agreement Form is now completed through an online Microsoft Form and the response is kept on the school's Arbor system.

Appendix A

Pupil and Parent/carers acceptable use agreements

The Acceptable Use Agreement Form is now completed through an online Microsoft Form and the response is kept on the school's Arbor system. Parents/carers sign to say they have read and agree with the guidance and will support the school and their child/ren in using IT responsibly.

In this section is the

Pupil Acceptable Use Agreements – KS2 Pupils and for EYFS/KS1 pupils
Parent/Carer Acceptable Use Agreement

Pupil Acceptable Use Agreement – KS2 Pupils

Charles Kingsley's C of E (VA) Primary School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that the pupils in our school will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement (Pupil) - Detailed

I will stay safe online.

- I will keep my username and password secret.
- I will never use someone else's login.
- I will not share my personal information online, such as my name, address, phone number or passwords.
- I will remember "**Clever Never Goes**" and never arrange to meet someone I only know online.
- I will tell a trusted adult straight away if I see or receive anything online that worries me, upsets me or makes me feel unsafe.

I will be kind and respectful.

- I will use kind and polite words when I communicate online.
- I will treat other people as I would like to be treated.
- I will not bully, upset or leave anyone out online.
- I will ask permission before taking or sharing photos or videos of other people.

I will use technology for learning.

- I will use school computers, iPads and the internet to help me learn.
- I will only use personal devices in school if a member of staff says I can.
- I will only visit websites and use apps that my teacher has approved.

I will look after school equipment.

- I will take care of computers, tablets and other devices.
- I will tell a teacher straight away if something is broken or not working properly.
- I will not change settings or install apps or software.

I will use the internet wisely.

- I will only open emails, links or attachments if a trusted adult tells me it is safe.
- I will not try to get around the school's internet filters.
- I will not search for, download or share anything that is unsafe, unkind or inappropriate.
- I will check that information I find online is true because not everything on the internet is accurate.

I will respect other people's work.

- I will not copy someone else's work and pretend it is my own.
- I will ask permission before using other people's pictures, music or videos.

I understand that my online behaviour matters.

- I know that the school helps keep everyone safe by monitoring the use of school devices and the internet.
- I understand that my behaviour online, both in and out of school, should be safe, kind and respectful.
- I know that if I do not follow these rules, the school may limit my use of technology, speak to my parents or carers and take further action if needed.

I promise to use technology safely, responsibly and respectfully so that everyone can enjoy learning online.

Child Friendly Version

I promise to use technology safely, responsibly and respectfully so that everyone can enjoy learning online – so I will:

- stay safe online.
- be kind and respectful.
- use technology for learning.
- look after school equipment.
- use the internet wisely.
- respect other people's work.

I understand that my online behaviour matters.

Pupil Acceptable Use Policy Agreement – for EYFS/KSI pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of devices and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules, I might not be allowed to use a device

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that the school and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

As the parent/carers, I give permission for my son/daughter to have access to the internet and to IT systems at school.

- I know that my son/daughter will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that the pupils will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

The responses to the completed Microsoft forms are securely stored in school's Arbor account. They may be accessed by the DSLs or the Online safety lead.

I promise to use technology
**safely, responsibly,
and respectfully...**



stay safe online.



use technology for learning.



look after school equipment.



be kind and respectful.



use the internet wisely.

**I understand that my online
behaviour matters.**

Online Safety

I promise to use technology safely, responsibly and respectfully so that everyone can enjoy learning online.



1. Stay safe online.
2. Be kind and respectful.
3. Use technology for learning.
4. Look after school equipment.
5. Use the internet wisely.
6. Respect other people's work.



I understand that my online behaviour matters!

I Promise

to use technology safely, responsibly and respectfully so that everyone can enjoy learning online – so I will:



- stay safe online.

- be kind and respectful.

- use technology for learning.

- look after school equipment.

- use the internet wisely.

- respect other people's work.



*I understand that my
online behaviour matters.*

This document is an **Online Safety Policy for Charles Kingsley's CE School**. It sets out how the school safeguards pupils, staff and the wider school community when using digital technology, in line with statutory guidance such as **Keeping Children Safe in Education 2026**, DfE filtering and monitoring standards, cyber security standards, UK GDPR and related safeguarding requirements.

Key points:

- **Online safety is treated as part of safeguarding and child protection.** The school takes a whole-school approach to protecting children from harmful or inappropriate online material and ensuring concerns are identified, reported, escalated and addressed.
- **Responsibilities are clearly allocated.** Governors approve and review the policy; the Headteacher/DSL has lead safeguarding responsibility; the Online Safety Lead supports policy, training and curriculum work; IT providers manage technical systems; staff, learners, parents and community users all have defined duties.
- **Filtering, monitoring and cyber security are central safeguards.** The school commits to maintaining secure systems, reviewing filtering and monitoring at least annually, checking effectiveness across devices, managing alerts, recording actions and ensuring appropriate escalation routes.
- **Staff must model safe and professional digital behaviour.** They are expected to use official school systems for communication, follow acceptable use agreements, report concerns promptly, supervise pupils' technology use, protect data and understand risks linked to AI, social media and online abuse.
- **Learners are taught to use technology safely and responsibly.** The curriculum covers topics such as online relationships, consent, abuse, misinformation, deepfakes, scams, harmful content, discrimination, reporting concerns, digital resilience and responsible use of AI.
- **AI use is addressed in detail.** The policy recognises the benefits of AI for teaching, learning and administration, but requires school-approved tools, anonymised data, UK GDPR compliance, transparency, human oversight, fact-checking and prompt reporting of misuse or incidents.
- **Parents and carers are involved.** The school aims to support families through policies, acceptable use agreements, newsletters, website information, workshops, awareness campaigns and opportunities to reinforce online safety messages at home.
- **Reporting systems must be clear and responsive.** Online safety incidents, including potentially illegal or harmful activity, must be reported through safeguarding procedures. Staff misuse is escalated appropriately, and serious concerns may involve external safeguarding routes.
- **Policies cover mobile phones, remote education, social media, digital images, online publishing and data protection.** The school promotes mobile-phone-free expectations for pupils, safe remote learning, careful use of images, protected publication of pupil work, and professional standards online.
- **The policy is reviewed regularly.** The Governing Body reviews it at least annually, considering emerging technologies, AI developments, filtering and monitoring, cyber security risks, safeguarding incidents, pupil voice, staff and parent feedback, and national/local guidance.

Overall, the policy presents online safety as a shared responsibility across the whole school community, combining education, safeguarding practice, technical protection, professional standards and ongoing review.

Appendix D

IT Resources and access updated yearly

CKS acknowledges the need to continually maintain, update and develop its resources and to make progress towards a consistent, compatible pc system by investing in resources that will effectively deliver the strands of the national curriculum and support the use of ICT and computing across the school. Teachers are required to inform the ICT and computing lead teacher of any faults as soon as they are noticed so that the PSD Schoolcare technician can deal with the issues remotely or during their half termly visits, the contact details for the Schoolcare helpline are displayed in each classroom. Resources if not classroom based are located in the Key Stage 1 corridor and the Year 6 work area. ICT and computing network infrastructure and equipment has been sited so that:

- every classroom from Cassatt to Da Vinci can have a laptop that is connected to the school network linked to an ActivPanel Titanium interactive display.
- there is a laptop set up permanently in the school hall.
- there is a laptop in the library linked to the library system
- SLT have laptops
- there are 4 desktops available for the office staff.
- there are laptops available for staff covering PPA so that the classroom laptops can be used by teachers for PPA task.
- there are two laptop trollies in school containing 32 laptops with internet access available to use in classrooms.
- there is one device trolley containing 32 iPads with internet access available to use in classrooms, as part of P.E. sessions and for outdoor learning.
- Cassatt class (YR), Matisse class (Y2) and Lowry class (Y1) have two iPads.
- there are class iPads for Year 3 through to Year 6, plus iPads for KS2 SNAs, Nurture and the office
- the Reception classrooms have two desktop computers.
- the laptops and iPads are available for use throughout the school day as part of computing lessons and for cross curricular use
- pupils may use technology devices independently, in pairs, alongside a LSA/SNA or in a group with a teacher
- through (PSD) Schoolcare the school has a technician that visits half termly or for specific needs (there is also a helpdesk available to do updates or changes remotely)
- a remote server so staff can access all documents remotely if needed through sharepoint and onedrive. These are linked and there for protected by their email accounts.