Chorlton C of E Primary School

Online Safety Policy

Ratified: October 2026
Review: October 2027
This Policy will be reviewed annually

Roles

Role	Name	Onsite/Offsite
Head teacher	Phil Trohear	Onsite
Online safety lead	Phil Trohear/Jo Derbyshire	Onsite
Computing Lead	Lauren Willetts	Onsite
Safeguarding governor	Sue Hilton	School affiliate
IT technician	Jonathan Hambleton HG IT	Offsite
Designated Safeguarding Leads (DSLs)	Phil Trohear, Vicki Foreman, Tom Butler, Claire Gunn, Laura Bethel, Jo Derbyshire	Onsite

Development, Monitoring and Review of this Policy

Schedule for development, monitoring and review

Task / Responsibility	Target / Detail
This policy was approved by the Governing Body	Friday 9th October 2026
Monitoring Group (Online safety lead / Senior Leadership Team / Safeguarding Governor)	The implementation of the online safety policy will be monitored by the Online Safety Lead, Senior Leadership Team, and Safeguarding Governor, with reports submitted to the Governing Body. The policy will be formally reviewed annually and additionally as soon as possible following any significant online safety incident or changes in legislation or technology. [Added by Google Gemini: Monitoring will also evaluate emerging risks including Generative AI and deepfake technologies.]
Monitoring Intervals	Every year for FGB in October
Reporting to Governing Body	The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: Every year for FGB in October

Task / Responsibility	Target / Detail
Review Schedule	The ONLINE safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: Every Autumn term

External Contact Points

Should serious online safety incidents take place, the following external persons/agencies should be informed: HG IT: 03333 583 950

Monitoring Tools

The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMS
- Automatic monitoring of logs of internet activity (including sites visited). These automatically forward concerns and inappropriate use to Headteacher (DSL) and HG IT via Smoothwall
- Automatic monitoring of computer network activity (HG IT)
- Surveys/questionnaires of pupils, parents/carers and staff.

Scope of the Policy

This policy applies to all use of school digital technology systems, whether accessed on-site or remotely (including home learning). Staff and pupils must adhere to the same standards of behaviour, safeguarding practices, and filtering compliance when accessing school systems off-site.

The Education and Inspections Act 2006 empowers Headteachers to regulate the behaviour of pupils off-site, including incidents of cyber-bullying or online safety breaches linked to school membership. The 2011 Education Act provides powers to search for/of electronic devices and delete data in accordance with the school Behaviour Policy.

Duties under the Counter Terrorism and Security Act 2015 require schools to protect children from terrorist and extremist material. Revised 'Keeping Children Safe in Education' (KCSIE 2026) guidance obliges schools to ensure robust, regularly audited filtering and monitoring systems are in place. [Added by Google Gemini: This includes addressing risks associated with generative artificial intelligence (AI), synthetic media, deepfakes, and automated content generation.]

This policy also governs emerging technologies, including Generative AI tools, dynamic machine-learning content creation, synthetic media, and deepfakes. This policy aligns with the latest OFSTED inspection framework (2025/2026), particularly safeguarding and leadership standards.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Safeguarding Governor and online safety will be overseen as part of this role. Safeguarding Governor meetings with the Head on safeguarding will also include:

- Online safety update
- Termly report of online safety incidents

- Termly report on changes to filtering and monitoring

Reporting at relevant Governors meetings on safeguarding by the Safeguarding Governor will include above information on online safety

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Leader.
- The Headteacher and Deputy will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see section on "Responding to incidents of misuse" P.14 and relevant Local Authority HR disciplinary procedures).
- The Senior Leadership Team will receive termly monitoring reports from the Online Safety Lead where online safety incidents have occurred.
- The Headteacher is responsible for ensuring that the Online Safety Leader and other relevant staff receive suitable training to enable them to carry out their Child Protection, Safeguarding and Online safety roles and to understand their expectations, roles and responsibilities around filtering and monitoring.
- The Headteacher and Senior Leadership Team must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. They will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable. This includes risk-assessing assistive digital technologies and AI platforms used by pupils with SEND.

Online Safety Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff.
- Ensures that online safety issues are documented on CPOMS, followed up and resolved in-line with school policies.
- May attend relevant meeting of Governors where serious concerns are highlighted from incident reports or developments in online safety have been made.
- Maintains up-to-date awareness of emerging risks, including generative AI threats, deepfake misuse, and automated digital harms.

Network Support Team / IT Technician

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and

ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct a full security check and monitoring the school's ICT systems.
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensure that any online safety incidents, including cyber-bullying, are logged and dealt with appropriately in line with this policy.
- Ensure technical safeguards continuously account for non-traditional content creation tools, such as Generative AI tools and unvetted third-party web apps.

Teaching and Support Staff

- They have an up to date awareness of online safety matters and of the current school online safety policy and procedures including their understanding of their expectations, roles and responsibilities around filtering and monitoring.
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA) (Appendix 3).
- They report any suspected misuse or problems by other adults to the Headteacher or Online Safety Lead for investigation.
- They log any Online Safety incidents relating to children on CPOMS.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems (Appendix 3).
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow this Online Safety Policy and pupil AUA (Appendices 1 and 2).
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations including appropriate and ethical use of AI tools.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where permitted) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites and/or materials checked as suitable for their use and that children and staff understand what they need to do if unsuitable material is found in internet searches.
- Where staff find unblocked harmful, extremist or illegal content they must report it to the Online Safety Lead.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).

Designated Safeguarding Leads (DSLs)

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- filtering and monitoring
- targeted online harassment, peer-on-peer abuse facilitated via generative AI, synthetic imagery, or deepfakes

Pupils

- Are responsible for using the school digital technology systems in accordance with the EYFS/KS1 or KS2 Pupil AUA (Appendices 1 and 2).

- Are responsible for gaining a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and to know how to do so: Turn off screen and report to responsible adult.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking of images, on the use of these images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school, as covered by the curriculum.
- Understand that the school's AUA covers their actions out of school, if related to their membership of the school (Appendices 1-2).
- When out of school, if accessing something that has been set up within school, such as email accounts, Google Classroom etc., school Online Safety policies apply, the curriculum content must be followed and AUA applies to their actions (Appendices 1-2).

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website, and information about national and local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and online pupil records

Community Users

Those who access school systems as part of the wider school provision will be expected to sign an AUA before being provided with access to school systems (Appendix 4).

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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:

- Online safety education is embedded within the Computing and PSHE curriculum and reinforced across all subjects. Staff receive guidance and training to ensure consistent delivery of online safety messages, and pupil understanding is regularly assessed and reflected upon in curriculum planning.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information [Added by Google Gemini: including evaluating AI-generated content, synthetic media, and fake news].
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Where pupils find unblocked harmful, extremist or illegal content they must report it to a senior member of staff.
- The AUA, signed annually by pupils and staff, covers inappropriate content which may include radicalisation and related extremist content (Appendices 1-3).
- Pupils should be helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use both within and outside school (Appendices 1-2).
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit by ensuring that screens of the children are visible to the managing staff, through good teaching practice, reminding children of their responsibility for whistle blowing on inappropriate or unsafe behaviour, and through the use of remote screen monitoring.

Education – parents and carers

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

- Curriculum activities
- 'Parent/Carer friendly' language on School website
- 'The school line' on current online safety issues on School website
- Parents and Carers evenings
- High profile events and campaigns e.g. Safer Internet Day
- Reference to the relevant websites and publications including parental guidance on generative AI, social media safety, and home filtering].

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and AUA (Appendix 3).
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. Learning outcomes are shared with staff and published on the website where appropriate.
- Online safety education and training materials are adapted to meet the needs of pupils and staff with SEND, ensuring accessibility and appropriate support to enable full participation.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The Online Safety Lead and/or the Computing Lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training and awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation, for example National Online Safety.
- Participation in school training and information sessions for staff or parents. This may include attendance at assemblies and lessons.

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be annual reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- The "administrator" passwords for the school ICT system, used by the network support staff must also be available to the Headteacher or Deputies and kept in a secure place (e.g. school safe).
- The Computing Lead is responsible for ensuring that software licenses are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.
- Internet access is filtered and monitored for all users. Illegal content (such as child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use (e.g. searches and web addresses) is logged and automatically monitored and concerns are forwarded to Safeguarding Designated Persons.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- We filter out social media, such as Facebook.
- IT staff will prevent further access when new sites that are unblocked are found.
- There is a process in place to deal with requests for filtering changes.
- Automatic monitoring and recording of the activity of users on the school technical systems flags concerning activity and routed to DPs. Users are made aware that their activity is monitored in the AUA (Appendix 1-4).
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed AUA is in place (Appendix 4) for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed AUA is in place (Appendix 3) regarding the extent of personal use that users (staff, pupils and community users) and their family members are allowed on school devices that may be used out of school.
- An agreed AUA is in place (Appendix 3) regarding the use of removable media (e.g. memory sticks, CDs and DVDs etc.) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured through an agreed system e.g. Google Drive.
- Staff are not allowed to download executable files onto school technology, though they can request that IT support staff do this for them. Any software [Added by Google Gemini: or Generative AI tool] used by children should be risk assessed.

Digital Images and Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites as well as the risks of image manipulation via AI image generators or deepfakes].
- 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 nor made publicly available on social networking sites or social messaging, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the AUA concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used (Appendices 3-4).
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. (For example, photos of children at a swimming gala would be considered inappropriate.)
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully by teachers and will comply with good practice guidance (only the first name of pupils should be used, there should be parent permission to use the image) on the use of such images.
- Pupils' 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 pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to The Data Protection Act 2018 and the UK GDPR.

The school must ensure that:

- It has a Data Protection Policy (https://chorlton-cofe-primary-school.secure-primarysite.net/data-protection/).
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- It provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice.
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see/to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary [Added by Google Gemini: including prior to the adoption of new digital tools, AI platforms, or cloud storage solutions].
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required

by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

Staff must ensure that:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school.
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Will not transfer any school/academy personal data to personal devices except as in line with school policy.

When personal data is stored on any portable computer system or removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

The use of removable media is not allowed for the storage of personal data unless it meets the above requirements.

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the appropriate person (the class teacher for children, or the Online Safety Lead for adults) – 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.
- Any digital communication between staff and pupils or parents / carers (email, chat, Virtual Learning Environment (VLE) etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Communication Technologies Summary

Technology / Activity	Staff: Allowed	Staff: Allowed with approval from SLT	Staff: Not allowed	Pupils: Allowed	Pupils: Allowed with staff approval	Pupils: Not allowed
Mobile phones may be brought to school	X			Yr6		X
Use of mobile phones in lessons			X			X
Use of personal mobile phones in social time	X					X
Taking photos on personal mobile phones/cameras			X			X
Use of other school mobile devices e.g. tablets, gaming devices	X				X	
Accessing personal email addresses in school or on school network	X					X
Use of school email for personal emails			X			X
Use of messaging apps on school devices			X			X
Use of social media on school devices			X			X
Use of blogs	X				X	

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff.
- They avoid posting any content on personal social media platforms that could potentially identify pupils or the school community. The school provides training on maintaining professional boundaries online and guidance on managing privacy settings to protect personal and professional reputations.
- 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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Protection from Harm

The internet provides children and young people with access to a wide online range of content, some of which is harmful. The range of harm covers the scope of material from inappropriate to extreme. Content is defined here as images, websites or parts of websites, advertising, videos, text or other material found on the web or accessed through the internet.

Inappropriate content is not suitable or proper in the circumstances for the user, (specifically taken in this policy to mean the user's age). Something that is appropriate for an older age group can be inappropriate for a younger age group.

Harmful content is content that is both inappropriate and harmful to the user. In the school context, we are here referring to content that is harmful to children. This harm includes emotional and psychological aspects. Cases which relate to physical harm are treated as illegal.

Extremist content is not allowed and should be reported to the police. Extremism is the vocal or active opposition to our fundamental British values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. We also regard calls for the death of members of the UK armed forces as extremist.

Illegal content as defined in UK law is unacceptable for all users. Any instance of criminal illegal content should be reported to the police.

Unsuitable / Inappropriate Activities

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to the following (refers to all users except where otherwise stated):

User Actions	Acceptable	Acceptable for staff on school business outside learning time	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 [Added by Google Gemini: including AI-generated synthetic imagery]					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
Possession of an extreme pornographic image (grossly offensive, disgusting or of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X

User Actions	Acceptable	Acceptable for staff on school business outside learning time	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Pornography				X	
Promotion of any kind of discrimination				X	
Threatening behaviour, including promotion of physical violence or mental harm				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading/uploading large files that hinders others use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing in line with AUA		X	X		
Use of social media on school devices				X	

User Actions	Acceptable	Acceptable for staff on school business outside learning time	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Use of messaging apps on school devices				X	
Use of video broadcasting e.g. YouTube			X		
[Added by Google Gemini: Unauthorised input of personal or sensitive data into third-party AI platforms]				X	

Responding to Incidents of Misuse

Children should immediately report any inappropriate, harmful, extremist or illegal content or behaviour to a supervising adult. The supervising adult should then handle the concern using the flowchart below.

Adults: any material or behaviour which an adult sees or finds that is inappropriate, harmful, extremist or illegal must be handled using the flowchart below.

Online safety Lead and DSLs are responsible for handling the incident in accordance with the incident response procedure.

Incident Response Matrix: Pupil Incidents

Incident Category	Refer to Teacher	Refer to head of phase / deputy	Refer to Head teacher	Refer to police	Refer to technical support staff	Inform parents/carers	Removal of network access	Warning	Further sanctioning (e.g. exclusion)
Deliberately accessing/trying to access illegal material		X	X	X		X	X		
Unauthorised use of non-educational sites in lessons	X	X				X			
Unauthorised use of mobile phone / digital camera	X	X				X		X	
Unauthorised use of social media / personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X				X		X	

Incident Category	Refer to Teacher	Refer to head of phase / deputy	Refer to Head teacher	Refer to police	Refer to technical support staff	Inform parents/carers	Removal of network access	Warning	Further sanctioning (e.g. exclusion)
Sharing username and passwords	X		X		X	X	X		
Accessing network using another student's account	X		X			X	X	X	
Accessing network using staff account	X	X	X			X	X	X	
Corrupting or destroying data of other users	X	X				X	X	X	
Sending offensive / harassing / bullying messages	X	X	X			X	X	X	
Continued infringements following warnings			X			X	X		X
Actions bringing school into disrepute		X	X			X	X	X	
Using proxy sites to subvert filtering		X	X		X	X	X	X	
Accidentally accessing offensive/pornographic material & failing to report	X	X	X		X	X			
Deliberately accessing/trying to access offensive/pornographic material	X	X	X		X	X	X	X	
Copyright or Data Protection Act breach	X	X				X	X	X	
[Added by Google Gemini: Generating, sharing, or creating abusive deepfakes/synthetic media]		X	X	X		X	X		X

Incident Response Matrix: Staff Incidents

Incident Category	Refer to Line manager	Refer to Head teacher	Refer to Local Authority/HR	Refer to police	Refer to technical support staff	Warning	Suspension	Disciplinary action
Deliberately accessing/trying to access illegal material		X	X	X		X		
Inappropriate personal use of internet / social media		X				X		
Unauthorised downloading or uploading of files		X				X		
Sharing account credentials / using another's account		X			X	X		
Careless use of personal data	X	X						
Deliberate breach of data protection or security rules		X	X			X		
Corrupting/destroying data or damaging hardware	X	X	X			X		X
Sending offensive / harassing / bullying messages	X	X			X	X		X
Using personal email/social media to contact pupils	X	X				X		X
Actions compromising professional standing	X	X				X		
Actions bringing school into disrepute	X	X				X		X
Using proxy sites to subvert filtering	X	X	X		X	X		X
Accidentally accessing offensive material & failing to report	X	X			X	X		

Incident Category	Refer to Line manager	Refer to Head teacher	Refer to Local Authority/HR	Refer to police	Refer to technical support staff	Warning	Suspension	Disciplinary action
Deliberately accessing offensive/pornographic material		X	X		X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements following warnings		X	X		X		X	X
[Added by Google Gemini: Inputting confidential pupil/staff data into unvetted AI systems]	X	X				X		X

Appendix 1: Acceptable Use Agreement (AUA): EYFS/KS1

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

- I will only use the internet when an adult is with me.
- I know the school can see what I am doing online.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe online.
- I will take care of computers/tablets and other equipment.
- I will ask for help from an adult if I am not sure what to do.
- I will ask for help from an adult 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 computer/tablet.

Appendix 2: Acceptable Use Agreement (AUA): KS2

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that school will filter and monitor my use of systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating online.
- I will not share personal information about myself or others when online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that school's systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission nor will I create or share edited/synthetic images of others.

I recognise that the school has a responsibility to maintain security and smooth running:

- I will not use my own personal devices (mobile phones etc.) in school.
- I understand the risks and will not try to upload, download or access any materials which are inappropriate or may cause harm or distress to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the sender.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that my access to devices/the internet may be taken away if I do not stick to this agreement.

Appendix 3: Acceptable Use Agreement (AUA): Staff and Volunteers

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

Acceptable Use Agreement:

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology.
- I will educate pupils in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that school will filter and monitor my use of school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies out of school, and to the transfer of personal data out of school.
- I understand that the school digital technology systems and devices are intended for educational use and that I will not use the systems/devices for personal or recreational use.
- I understand that all devices must be password protected and I will not disclose my username or password to anyone else. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I understand that personal devices should not be used in class. Specifically, mobile phones must not be on your person and should be stored (on silent) in a bag, cupboard or secure space. Mobile phones (and other personal devices) should only be used during breaks or PPA in the staffroom and when children are not present.
- I understand that photos, videos or sensitive data must not be taken or stored on personal devices.
- I understand that the use of USB or other portable storage devices (used to transfer data) is prohibited.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will immediately report any concerns regarding inappropriate use of personal data and/or any breach of the Data Protection Act 2018 and/or UK GDPR to the Data Controller (School Business Manager).

I will be professional in my communications and actions when using school 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 digital/video images. I will not use my personal equipment to record these images.
- Where these images are published on the school website I will ensure it will not be possible to identify by full name, or other personal information, those who are featured.
- I will only communicate with pupils and parents/carers using official school systems (professional email account, Seesaw). Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- [Added by Google Gemini: I will not enter any confidential, sensitive, or personal data concerning pupils or staff into unapproved AI tools or third-party web services.]

The school and the local authority have the responsibility to provide safe and secure access:

- I will not open any hyperlinks in emails or attachments unless the source is known and trusted.
- I will ensure that my data is regularly backed up and saved in an appropriate location.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage (through misuse or neglect) 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 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 data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when required by law or school policy to disclose 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 permission to use the original work of others in my own work.
- Where work 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 AUA applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises.
- I understand that if I fail to comply with this AUA, I could be subject to disciplinary action. This could include a warning, a suspension, disciplinary action and in the event of illegal activities the involvement of the police.

Appendix 4: Acceptable Use Agreement (AUA): Parents/Carers

At Chorlton C of E Primary School, we provide access to the Internet through an approved service provider. The service provider monitors and filters the sites available, to control the materials and the language available to children. As with any electronic monitoring system we do not have total control and have therefore put into place the below rules to further protect the safety of children using the Internet. These rules are shared with children in the form of an AUA and the wider themes of online safety and digital awareness are regularly taught as part of our Computing curriculum.

- Pupils must ask permission to use the Internet and may do so only in the presence of an adult.
- Pupils are expected to be responsible for their own behaviour on the Internet, just as they would in any area of the school. This includes the materials they choose to access or share and the language they use.
- Pupils are not expected to deliberately seek out sites that could cause offence.
- Should pupils accidentally encounter such materials or receive mail that causes concern, they should report this immediately to a teacher. The service provider will be notified.
- The school have the right to check pupil's files and monitor sites that have been visited. Any instances where inappropriate online materials are sought out are automatically logged by the school firewall system.
- Pupils should not give out personal information, pictures or the name and location of the school, unless part of an agreed school project.
- Pupils should only use the school devices for work related to school.
- Pupils must not use USB or other data storage devices from outside school without permission.
- Social networking sites, such as (but not limited to) Facebook, TikTok or Twitter, are prohibited for children under the age of 13.

Consent & Permissions

- I give permission for my child to use the Internet in school: [Yes] / [No]
- I give permission for photographs of my child to be published on the school Twitter account: [Yes] / [No]
- I give permission for photographs of my child to be published on the school website: [Yes] / [No]
- I give permission for photographs of my child, when in an individual setting, to be published on Seesaw and assigned to my child's learning journey: [Yes] / [No]
- I give permission for photographs of my child, when in a group/whole class setting, to be published on Seesaw and assigned to the specific group members and/or the whole class learning journey: [Yes] / [No]

If you have selected "no" to permissions 2 and 4, the school will ensure your child is not identifiable by covering their face before uploading/publishing.

Parent/Carer Declaration

To further protect the privacy of our children we ask all parents to provide positive confirmation to the below statements and act in accordance with them at all times.

As a parent/carer I will:

- Not take screenshots or publish any of my child's observations, photographs or videos on any social media platform [Added by Google Gemini: nor use digital tools or AI to edit, alter, or share images of pupils from school platforms].
- Ensure any comments I add to pictures, videos or other work posted on Seesaw are appropriate in both language and content.
- Keep any login details, provided by school, within my trusted family.
- Contact school via email (admin@chorlton.manchester.sch.uk) if I have any queries regarding any of the content of this form.