Online Safety and Acceptable Use of Technology Policy

Agreed: April 2024

Key Details

Designated Safeguarding Lead (DSL): Charlotte Mulhall

Named governor with lead responsibility: Karen Seddon

Date written: February 2024

Date agreed and ratified by the governing body: (March, 2024)

Date of next review: Spring 2025

This policy will be reviewed at annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Cranwell Primary School Online Safety Policy

Intent

Our School's Intent is to safeguard children from potentially harmful online material and to teach them how to keep themselves safe online. Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. We aim to empower and educate pupils and our wider community in their use of technology and establish mechanisms to identify, intervene and escalate any concerns where appropriate.

Policy Aims

This online safety policy has been written by Cranwell Primary School, involving staff, pupils and parents/carers.

It takes into account the most recent DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage statutory framework, 'Working Together to Safeguard Children' 2023 'Education for a Connected World' 2020 and the local Safeguarding Children Multi-agency Partnership procedures.

The purpose of Cranwell Primary School's Online Safety policy is to:

- safeguard and promote the welfare of all members of Cranwell's community online
- identify approaches to educate and raise awareness of online safety throughout our community
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- identify clear procedures to follow when responding to online safety concerns.

Cranwell Primary School understands that the issues associated with online safety are considerable but can be broadly categorised into three areas of risk:

1. **Content:** being exposed to illegal, inappropriate or harmful material.
2. **Contact**: being subjected to harmful online interaction with other pupils.
3. **Conduct:** personal (staff or pupils) online behaviour that increases the likelihood of, or causes, harm.
4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Policy Scope

Cranwell Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.

Cranwell Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks.

Cranwell Primary School will empower our pupils to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers, employees of ARK ICT and other individuals who work for, or provide services on behalf of the setting (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

This policy applies to all access to the internet and use of technology, including mobile technology, or where pupils, staff or other individuals have been provided with setting issued devices for use, both on and off site.

Links with other Policies and Practices

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable Use Agreements
- Code of Conduct policy
- Staff Disciplinary policy
- Behaviour and Discipline policy
- Safeguarding and Child Protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education & Relationships and Sex Education (PSHE & RSE),
- Data Protections policy

Monitoring and Review

Technology evolves and changes rapidly and, as such, Cranwell Primary School will review this policy annually. The policy will be revised following any national statutory guidance or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure oversight of online safety, the Headteacher, DSL and Computing Lead will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will oversee and report, with the DSL, online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

Any issues identified via monitoring policy compliance will be incorporated into our action planning.

Part 1 – Pupils

Roles and Responsibilities

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

- engage in age/ability-appropriate online safety education
- contribute to the development of online safety policies
- read and adhere to the Acceptable Use of Technology and Behaviour policies
- respect the feelings and rights of others, on and offline
- take an appropriate level of responsibility for keeping themselves and others safe online
- seek help from a trusted adult, if they are concerned about anything they or others experience online.

Education and Engagement

We will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst pupils by:

- ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance
- ensuring online safety is addressed in our RSE, PSHE and Computing programmes of study
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site
- creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online
- involving the DSL, as appropriate, as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content
- making informed decisions to ensure that any educational resources used are appropriate for our pupils
- using external visitors, where appropriate, to complement and support our internal online safety education approaches
- providing online safety education as part of the transition programme across the key stages and/or when moving between establishments

Cranwell Primary School will support pupils to understand and follow our Acceptable Use Agreements in a way which suits their age and ability by:

- displaying acceptable use posters in all rooms with internet access
- informing pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation
- seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

Cranwell Primary School will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age-appropriate education regarding safe and responsible use precedes internet access
- teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation

- enabling them to understand what acceptable and unacceptable online behaviour looks like
- preparing them to identify possible online risks and make informed decisions about how to act and respond
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Pupils

Cranwell Primary School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage, and personal circumstances. However, there are some pupils, for example Looked After Children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.

Cranwell Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable pupils.

Staff at Cranwell Primary School will seek input from specialist staff as appropriate, including the DSL and SENCO to ensure that the curriculum is adapted to our community's needs.

Technical Security – Passwords

A safe and secure username/password system is essential if the above is to be established, and this applies to all school technical systems, including networks and devices.

Pupil passwords

All pupils in Cranwell Primary School will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of pupils will be recorded by the Network Manager (ARK).

Passwords for new pupils, and replacement passwords for existing pupils, will be allocated by the Network Manager. Pupils will be taught the importance of password security and how to choose a strong password.

All pupils (adults and young people) will have responsibility for the security of their username and password, and must not allow other adults or pupils to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security.

All pupils will be provided with a username and password by the Network Manager who will keep an up-to-date record of pupils and their usernames.

Filtering and Monitoring

Internet access is filtered for all pupils. At Cranwell Primary School, if pupils become aware of any infringements or abuse of the Schools's filtering systems, they must report this immediately to their class teacher, Headteacher or DSL.

Pupils will not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place.

Using and Publishing Images and Videos Online

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, all Cranwell Primary School community need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term.

Guidance

Pupils will be advised about the risks associated with the taking, use, sharing, publication and distribution of images. They will be encouraged to recognise the risks attached to publishing their own image on the internet, e.g. on social networking sites. Pupils will not take, use, share, publish or distribute images of others without their permission.

Managing Email

Pupils may use a provided email account for educational purposes. Pupils will agree an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

Social Media

Expectations

The expectations regarding safe and responsible use of social media applies to all members of Cranwell Primary School community including pupils.

The term 'social media' may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.

All members of Cranwell Primary School community are expected to engage in social media in a positive and responsible manner.

Pupils should not post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

Concerns regarding the online conduct of any member of our school community on social media will be reported to the DSL or Headteacher without delay and be managed in accordance with our Anti-bullying, Staff Code of Conduct, and Safeguarding policies.

Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites and resources.

Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including Safeguarding, Anti-bullying, and Behaviour policies.

Concerns regarding pupils' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Pupils will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present
- to use safe passwords
- to use social media sites which are appropriate for their age and abilities
- how to block and report unwanted communications
- how to report concerns on social media, both within the setting and externally.

Mobile Technology – Use of Mobile Phones and Personal Devices

Expectations

Cranwell Primary School recognises that personal communication through mobile technologies is part of everyday life for many pupils however mobile technology, including mobile phones and personal devices such as tablets, games consoles and wearable technology are not permitted in school. Electronic devices of any kind that are brought onto site with consent between school and parents must be stored securely with the class teacher at the start of the school day and returned at the end of the school day.

Watches with the capability to voice record and take photographs are not permitted in school.

Concerns About Online Behaviour and/or Welfare

All concerns about pupils will be recorded in line with our Safeguarding policy. The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks.

Cranwell Primary School recognises that while risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online child-on-child abuse concerns will be responded to in line with our Safeguarding and Behaviour policies.

The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

Appropriate sanctions and/or pastoral/welfare support will be offered to pupils as appropriate.

We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Part 2 – Staff/Adults

Roles and Responsibilities

The Headteacher and DSL have responsibility for online safety. While activities of the DSL may be delegated to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with them.

Cranwell Primary School recognises that all members of the community have important roles and responsibilities with regards to online safety.

The Leadership and Management Team will:

- create a culture that incorporates online safety throughout all elements of school life
- ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- implement appropriate and up-to-date policies regarding online safety, which address the acceptable use of technology, child-on-child abuse, use of social media and mobile technology.
- Work with technical staff support to ensure that suitable and appropriate filtering and monitoring systems are in place
- support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities

- ensure robust reporting channels are in place for the whole community to access regarding online safety concerns
- undertake appropriate risk assessments regarding the safe use of technology on site
- audit and evaluate online safety practice to identify strengths and areas for improvement
- ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety
- support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all pupils to develop an appropriate understanding of online safety.

The DSL will:

- act as a named point of contact within the setting on all online safeguarding issues
- liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety
- ensure appropriate referrals are made to relevant external partner agencies, as appropriate
- work alongside staff to ensure online safety is recognised as part of the school safeguarding responsibilities, and that a coordinated whole school approach is implemented
- access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online.
- access regular and appropriate training and support to ensure the school recognises the additional risks that pupils with SEN and disabilities (SEND) face online
- ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training
- keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate
- ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches, including workshops, training and individual support
- maintain records of online safety concerns, as well as actions taken, as part of the setting's safeguarding recording mechanisms, relating to both adults and pupils
- monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures
- work with the leadership team to review and update Online Safety policies on a regular basis (at least annually) with stakeholder input
- meet regularly with the school IT technician and the governor with a lead responsibility for safeguarding and/or online safety.

It is the responsibility of all members of staff to:

- read and adhere to the Online Safety policy and Acceptable Use of Technology Agreements
- understand that sanctions may apply for breaches of acceptable use, which may include following school disciplinary procedures
- take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally
- take responsibility for the security of IT systems and the electronic data they use or have access to
- model good practice, in line with policy, when using technology with pupils
- maintain a professional level of conduct in their personal use of technology, both on and off site
- embed online safety education in curriculum delivery wherever possible
- have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care
- identify online safety concerns and take appropriate action by following the school Safeguarding policies and procedures

- know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally
- take personal responsibility for professional development in this area
- where appropriate, contribute to the development of our Online Safety policies
- ensure that any IT equipment taken from the school site is properly managed and kept securely. Ensure no overnight storage of IT equipment in cars
- ensure any data covered by GDPR is kept secure.
- All computers must be secured by a Bitlocker and a strong password that is different to other devices.

Education and Engagement

We will:

- provide and discuss the Online Safety policy and procedures with all members of staff as part of induction
- provide up-to-date and appropriate online safety training (annually) for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach.
- Staff training covers the potential risks posed to pupils (content, contact, conduct and commerce) as well as our professional practice expectations.
- Build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual staff and pupils. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role, reputation and could result in disciplinary procedures in line with Staff Code of Conduct Policy
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.

Reducing Online Risks

Cranwell Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate checks before their use in the school is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and, as such, identify clear procedures to follow if breaches or concerns arise.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our Acceptable Use of Technology Agreements and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom use

Cranwell Primary School uses a wide range of technology. This includes access to:

- computers, laptops, tablets and other digital devices
- internet, which may include search engines and educational websites learning platform/intranet
- email
- digital cameras, web cams and video cameras.

All setting-owned devices will be used in accordance with our Acceptable Use of Technology Agreement and procedures, and with appropriate safety and security measures in place. Adults must adhere to these procedures at all time.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at school and home.

Member of staff must view content prior to sharing it with pupils.

We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.

Supervision of internet access and technology use will be appropriate to pupils' age and ability.

- Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupil's age and ability. Pupils will use age-appropriate search engines under direct supervision.
- Throughout EYFS and KS1 school owned ipads will be used to evidence work through photographs and videos and uploaded to Tapestry. These ipads should be 'staff only' and passcode protected. Staff members are responsible for logging out of tapestry when they have finished using it.

- Key Stage 2

- Pupils will use age-appropriate search engines and online tools.
- Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupil's age and ability.
- Throughout KS2 school owned ipads will be used to evidence work through photographs and videos. These ipads should be 'staff only' and passcode protected.

Password Security

Staff passwords:

- All staff will be provided with a username by the Network Manager who will keep an up-to-date record of staff and their usernames.
- The password should be a minimum of eight characters long and must include three of the following – uppercase character, lowercase character, number, special characters.
- It should not include proper names or any other personal information about the user that might be known by others.
- Temporary passwords, e.g. used with new user accounts or when pupils have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords will not be displayed on screen and shall be securely hashed (use of one-way encryption).

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the school. Passwords should be changed periodically. Passwords will not be re-used for six months, so passwords cannot be re-used passwords created by the same user.

Filtering and Monitoring

The filtering of internet content provides an important means of preventing pupils from accessing material that is illegal or inappropriate. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. Filtering is only one element in a larger strategy for online safety and acceptable use. Cranwell Primary School recognises that it is important that we have a filtering process to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Staff and adults at Cranwell Primary School have a responsibility to report immediately to the Headteacher/DSL/Computing Lead/Network Manager any infringements of the school's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered.

Staff/adults will not attempt to use any programmes or software that might allow them to bypass the filtering/ security systems in place.

Differentiated internet access is available for staff and customised filtering changes are managed by the Network manager. Illegal content is filtered by the broadband or filtering provider, by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and monitored through Securly filter console. The monitoring process alerts the school to filtering breaches, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. The school regularly reviews and logs the effectiveness of the filtering system, this is carried out at least termly.

Commented [GU1]: correct spelling!

Managing the Safety of the School Website

We will ensure that information posted on our website meets the requirements as identified by the DfE and ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

Staff or pupils' personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Using and Publishing Images and Videos Online

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They will be encouraged to recognise the risks attached to publishing their own image on the internet, e.g. on social networking sites.

For the safety of the pupils, parents/carers are asked not to take videos and digital images of their children at school events.

Staff can take digital/video images to support educational aims, but will follow school procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff must not be used for such purposes. Photos should be erased from any portable devices after a 12 month period.

Care will 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.

Photographs published on our website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Staff will not use pupils' full names anywhere on a website or blog, particularly in association with photographs.

Staff must obtain written permission from parents or carers before photographs of pupils are published on the school website or social media channels (e.g. Facebook and Twitter).

Pupils' work will only be published with the permission of the pupil and parents or carers.

School and Staff Email

All members of staff are provided with an email address which must be used for all official work-related communication. The use of personal email addresses by staff for any official business is not permitted.

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including the Confidentiality, Acceptable Use Agreements and the Staff Code of Conduct Policy.

Staff must ensure any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

Setting email addresses and other official contact details will not be used to set up personal social media accounts.

Members of the community will immediately tell the Headteacher and DSL if they receive offensive communication, and this will be recorded.

Social Media

Expectations

The expectations regarding safe and responsible use of social media applies to all members of Cranwell Primary School community, staff and pupils. All members of Cranwell Primary School community are expected to engage in social media in a positive and responsible manner.

The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.

All members of our community should not post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control access to social media while using device and systems provided by Cranwell Primary School on site.

Concerns regarding the online conduct of any member of our school community on social media will be reported to the DSL without delay and be managed in accordance with our Anti-bullying, Staff Code of Conduct and Safeguarding policies.

Use of social media

School staff will ensure that:

- staff do not post or communicate disparaging or defamatory statements using social media or otherwise about:
- our employees
- our governors
- our pupils and their parents/carers
- our suppliers, agents and contractors
- or statements that could be construed as being damaging or detrimental to the reputation of the school

- staff do not engage in disparaging online discussion on personal or professional matters relating to members of the school community. This includes the use of WhatsApp groups or other social media sites
- staff are personally responsible for what they communicate via social media and that what they publish might be read by an audience wider than they intended
- that any social media communication is shared on their own behalf and does not appear to be linked with the school in any way
- personal opinions will not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- any electronic or text communication should be conducted through the school's communication systems
- staff do not have any present pupils or those that have left less than six years ago as 'friends', except relatives. However, if there is a legitimate reason for such communication, such as involvement with relevant clubs such as Scouts, Youth Club or Football, then this should be declared to the Headteacher and a copy of that organisation's Safeguarding policy should be provided
- the expectations apply whether or not social media is accessed using school facilities and equipment or equipment belonging to staff personally and to the use of social media for both school and personal purposes, whether or not during working hours or otherwise
- the school's use of social media for professional purposes will be checked regularly by the Headteacher/DSL/Online safety Lead to ensure compliance with data protection, Online Safety and Safeguarding policies.

Unsuitable/inappropriate activities

Cranwell Primary School believes that the activities referred to in the following section would be inappropriate in an school context and that users, as defined below, will not engage in these activities in our school or outside when using school equipment or systems.

The school policy restricts usage as follows:

User Actions -Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: Child sexual abuse images – The making, production or distribution of indecent images of children – contrary to The Protection of Children Act 1978

- Grooming, incitement, arrangement or facilitation of sexual acts against children – contrary to the Sexual Offences Act 2003
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) – contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986
- Pornography

Promotion of any kind of discrimination

- Threatening behaviour, including promotion of physical violence or mental harm
- 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
- Using school systems for personal gain, e.g. to run a private business or accessing information for non-work-related matters
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- Online gaming (educational)
- Online gaming (non-educational)
- Online gambling
- Online shopping/commerce
- File sharing
- Use of social media
- Use of messaging apps
- Use of video broadcasting, e.g. YouTube

Official use of social media

Cranwell Primary School's official social media channels are: Twitter and Facebook

The official use of social media sites by Cranwell Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes.

The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher. Selective staff have access to account information and login details for our social media channels.

Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

Official social media use will be conducted in line with existing policies, including but not limited to Anti-bullying, Data Protection (GDPR), Confidentiality and Safeguarding.

All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Parents/carers will be informed of any official social media use with pupils; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Streaming Media and Related Sites

‘Streaming’ is the method for which media content, most commonly video and audio, is delivered to an end-user. The media is stored on one computer or server and, via the Internet, played back on another. Streaming media is not downloaded and stored on the receiving computer as a whole file, but is typically viewed on demand via a web page. YouTube and Vimeo are examples of popular streaming media websites.

Cranwell Primary School recognises that teaching can be enriched by the use of streaming media in the classroom. However, there are many identified risks associated with this type of content.

As a member of staff using streaming media in the classroom you will be expected to adhere to the following guidelines:

Acceptable Use

- The primary purpose for using streaming media is to enhance teaching and learning within the school. Streaming Media must only be used for legitimate teaching purposes, personal use is prohibited.
- Media content should be viewed from start to finish and a full assessment made of its suitability for the intended audience. The content should be considered in the same way that you would consider any other resources used in your classroom.
- Content must be assessed away from the view and earshot of students, preferably in a staff room or similar. Many classroom PC’s are connected to interactive whiteboards and projectors, and may be configured for whole class display. This must be considered when reviewing content.
- Where a resource is deemed appropriate for use, it is recommended that it is downloaded and saved for future use. This will prevent any issues with online content being removed or changed. Separate tools are required to download streaming media to a PC, and examples are available on the Intranet.
- If it is not possible to download the resource then the video should be viewed prior to each use, to ensure it remains suitable for the intended purpose.

Unacceptable Use

It is deemed inappropriate to view, create, access, download or publish material that is:

- Pornographic or Adult
- Racist, offensive, or derogatory
- Obscene
- Bullying
- Violent
- Fraudulent
- Likely to cause harassment to others
- Confidential
- Prejudicial to the school’s or Council’s best interests
- Not relevant to the business of the school or Council
- Likely to irritate or waste time of others
- Likely to breach copyright

It is accepted that the teaching of certain subjects may present the need to use resources that could fall into one or more of the above categories. In such situations it is expected that the subject matter is presented in context; in a sensitive; balanced manner; and is appropriate for the age of the intended audience.

It is also expected that any home / school contracts regarding religion, sex education, parental wishes etc are considered when selecting media content.

Mobile Technology – Use of Mobile Phones and Personal Devices and use of cameras (including smart watches)

Cranwell Primary School recognises that personal communication through mobile technologies is part of everyday life for many pupils, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as Confidentiality, Safeguarding, Data Protection and Acceptable Use policies.

Personal mobile devices should not be used during any face-to-face time with the pupils.

Staff will need personal mobile phones to access the multi-factor authentication for the school safeguarding system/ verify emails.

Staff and pupils may use mobile phones to monitor health conditions e.g. diabetes.

Mobile phones maybe used for emergency contact with other members of staff via phone call or messaging.

Staff must not take photographs on personal devices, including wearable technology.

A mobile phone will be taken on off site visits as emergency contact. Staff must not share their personal mobile numbers, with the exception of a school trip where an emergency contact may be needed.

The school has a communication group which must be used professionally and in accordance with all other policies.

Staff will be advised to:

- keep mobile phones and personal devices in a safe and secure place during lesson time
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times and not on their person
- not use personal devices during teaching periods, unless permission has been given by the Headteacher such as in emergency circumstances
- ensure that any content bought onto site via mobile phones and personal devices is compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents/carers. Any pre-existing relationships which could undermine this will be discussed with the DSL (or deputy) and the Headteacher.

Staff will not use personal devices or mobile phones:

- to take photos or videos of pupils and will only use work-provided equipment for this purpose
- communicate directly with pupils and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with the Disciplinary Policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our Managing Allegations Against Staff policy.

<u>Officially provided devices</u>

Some members of staff will be issued with a work email address, where contact with pupils or parents/carers is required.

Cranwell Primary School devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff. School devices will always be used in accordance with the Acceptable Use of Technology Agreement and other relevant policies.

Responding to Online Safety Incidents

All members of Cranwell Primary School community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, child-on-child abuse, including cyberbullying and youth-produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content. Members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and pupils to work in partnership with us to resolve online safety issues.

After any investigations are completed, the leadership will debrief, identify lessons learnt and implement any policy or curriculum changes, as required. If a member of staff has been dismissed for gross misconduct as a result of the misuse of devices or the internet, then the Headteacher will inform the Disclosure and Barring Service following the completion of the disciplinary process and in the case of a teacher, the TRA.

If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the LADO. Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

If information relating to a specific incident or a concern needs to be shared beyond our community, for example, if other local settings are involved or the wider public may be at risk, the DSL and/or Headteacher will speak with the police and the LA Safeguarding team first, to ensure that potential criminal or child protection investigations are not compromised.

Concerns about staff online behaviour and/or welfare

Any complaint about staff misuse will be referred to the Headteacher, in accordance with our Managing Allegations Against Staff Policy.

Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

Appropriate disciplinary, civil and/or legal action will be taken in accordance with the Staff Code of Conduct and Disciplinary Procedure. Welfare support will be offered to staff as appropriate.

Procedure for Responding to Specific Online Safety Incidents

Online sexual violence and sexual harassment between children

Our Headteacher, DSL and appropriate members of staff have accessed and understood the DfE 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' (2021) guidance and Part 5 of the latest guidance in 'Keeping Children Safe in Education'. Full details of our response to child-on-child abuse, including sexual violence and harassment can be found in our Safeguarding policy.

Cranwell Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- online coercion and threats
- 'up skirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
- unwanted sexual comments and messages on social media
- online sexual exploitation
- Sexual 'jokes'.

Cranwell Primary School will always respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- immediately notify the DSL (or deputy) and act in accordance with our Safeguarding and Anti-bullying policies
- if content is contained on pupils' personal devices, they will be managed in accordance with the latest DfE 'Searching, Screening and Confiscation at School' advice
- provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support
- implement appropriate sanctions in accordance with our behaviour policy
- inform parents/carers, if appropriate, about the incident and how it is being managed
- if appropriate, make referrals to partner agencies, such as children's social care and/or the police
- if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
- Refer to KCSE '23 part 5- The immediate response to a report.

If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised and review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Cranwell Primary School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, we will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age- and ability-appropriate educational methods as part of our curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between pupils.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

Cranwell Primary School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our Safeguarding policy.

Cranwell Primary School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target pupils, and understand how to respond to concerns.

We will implement preventative approaches for online child abuse and exploitation via a range of age- and ability-appropriate education for pupils, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

If made aware of an incident involving online child abuse and/or exploitation, we will:

- act in accordance with our Safeguarding policies and the relevant local safeguarding partnership procedures
- store any devices containing evidence securely
- if appropriate, make a referral to Lincolnshire children's social care and inform the police via 101, or 999 if a learner is at immediate risk
- carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate
- provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support
- review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school or personal equipment.

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Lincolnshire Childrens Services and/or police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).

If members of the public or pupils at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or Lincolnshire Children's services safeguarding team before sharing specific information to ensure that potential investigations are not compromised.

Indecent images of children (IIOC)

Cranwell Primary School will ensure that all members of the community are made aware of the possible consequences of accessing IIOC as appropriate to the age and ability.

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using appropriate filtering, firewalls and anti-spam software which is reviewed termly.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding team.

If made aware of IIOC, we will:

- act in accordance with our Safeguarding policy and the relevant local safeguarding partnership procedures
- store any devices involved securely
- immediately inform the police if a crime may have been committed.

If made aware that a member of staff or a learner has been inadvertently exposed to IIOC, we will:

- ensure that the DSL (or deputy) and ARK IT are informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk or blocked immediately by ARK
- ensure that any copies that exist of the image, for example in emails, are deleted
- report concerns, as appropriate to parents/carers
- Inform parents.

If made aware that IIOC have been found on the setting provided devices, we will:

- ensure that the DSL (or deputy) and Headteacher are informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk
- inform the police via 101 or 999 if there is an immediate risk of harm, and children's social services, as appropriate
- only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police
- report concerns, as appropriate to parents/carers.

If made aware that a member of staff is in possession of IIOC on Cranwell Primary School-provided devices, we will:

- ensure that the Headteacher is informed in line with our Managing Allegations Against Staff policy
- inform the Local LADO, and other relevant organisations in accordance with our Managing Allegations Against Staff policy
- quarantine any devices until police advice has been sought.

Staff should take extreme care to ensure that children and young people are not exposed, through any medium, to inappropriate or indecent images.

There are no circumstances that will justify adults: making, downloading, possessing or distributing indecent images or pseudo-images of children (child abuse images). Accessing these images, whether using the school's or personal equipment, on or off the premises, or making, storing or disseminating such material is illegal.

If IIOC are discovered at the school or on the school's equipment, an immediate referral should be made to the Local Authority Designated Officer (LADO) and the police contacted if relevant. The images/equipment should be secured and there should be no attempt to view or delete the images as this could jeopardise necessary criminal action. If the images are of children known to the school, a referral should also be made to children's social services in line with local arrangements.

Under no circumstances should any adult use school equipment to access pornography. Personal equipment containing pornography or links to it should never be brought into or used in the workplace. This will raise serious concerns about the suitability of the adult to continue working with children and young people.

Staff should keep their passwords confidential and not allow unauthorised access to equipment.

Cyberbullying

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

Online hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Cranwell Primary School and will be responded to in line with existing policies, including Safeguarding, Anti-bullying and Behaviour policies.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding team and/or the police.

Online radicalisation and extremism

As listed in this policy, we will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a pupil or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our safeguarding policy.

If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Safeguarding and Allegations policies.

Breaches

At Cranwell Primary School, we understand that we have a duty of care to provide a safe learning environment for pupils and staff. We could be held responsible, indirectly, for the acts of employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. As a result, we will act to address any infringements of this policy with urgently.

National links and resources for staff/adults

- CEOP: www.thinkuknow.co.uk www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Report Harmful Content: https://reportharmfulcontent.com/
- Childnet: www.childnet.com
- Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
- Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- NSPCC: www.nspcc.org.uk/onlinesafety

- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

Part 3 - Parents/Carers

Roles and Responsibilities

It is the responsibility of parents/carers to:

- read our Acceptable Use of Technology policies and encourage their children to adhere to them
- support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media and abide by the Home-School Agreement and Acceptable Use of Technology policies
- seek help and support from the school or other appropriate agencies, if they or their child encounter online issues
- contribute to the development of our Online Safety policies
- use our systems and other IT resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

Education and Engagement

Cranwell Primary School recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible pupils of the internet and associated technologies.

We will build a partnership approach to online safety with parents/carers by:

- providing information and guidance on online safety in a variety of formats- This will include offering specific online safety awareness training and regular updates via Parentmail, our website, social media channels and newsletters
- requesting parents/carers read online safety information as part of joining our community, for example, within our Home-School Agreement
- requiring them to read our Acceptable Use policies and discuss the implications with their children.

Use and Publishing Images and Videos Online

Parents/carers are asked not to take videos and digital images of their children at school events. Parents/carers will not upload or add any images, videos, sounds or text that could upset, threaten the safety or offend any member of the school community.

Mobile Technology – Use of Mobile Phones and Personal Devices

- Parents/Carers should ensure that mobile phones are not used whilst in the presence of any pupils other than their own
- Appropriate information is provided to inform parents/carers of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our Acceptable Use Agreement and other associated policies, including but not limited to Anti-bullying, Behaviour, and Safeguarding.
- Members of staff are expected to challenge parents/carers if they have concerns and inform the DSL (or deputy) of any breaches of our policy.

Concerns about Parent/Carer Online Behaviour and/or Welfare

Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher and/or DSL (or deputy). The Headteacher and/or DSL will respond to concerns in line with existing policies.
Civil or legal action will be taken if necessary.
Welfare support will be offered to parents/carers as appropriate.

National links and resources

- Parent Zone: https://parentzone.org.uk
- Parent Info: https://parentinfo.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Get Safe Online: www.getsafeonline.org

Part 4 – Visitors

Roles and Responsibilities

It is the responsibility of visitors to:

- read our acceptable use of technology agreements and to adhere to them
- role model safe and appropriate use of technology and social media and abide by Acceptable Use of Technology Agreement
- seek help and support from the School, if they encounter online issues
- use our systems and other IT resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies.

Mobile Technology – Use of Mobile Phones and Personal Devices

- Visitors, including volunteers and contractors, should ensure that mobile phones are not used whilst in the presence of children

- Appropriate signage and information are provided to inform parents/carers and visitors of expectations of use.

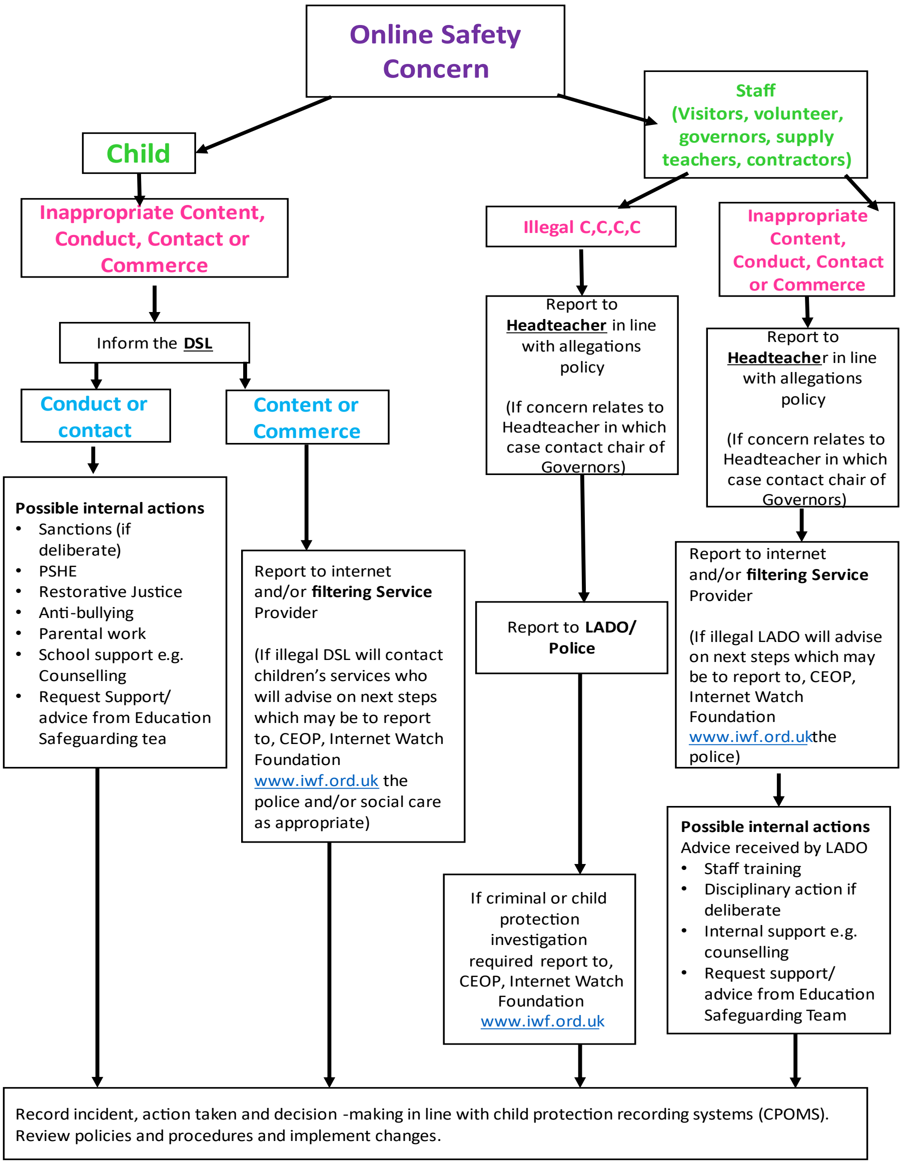
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our Acceptable Use Agreement and other associated policies, including but not limited to Anti-bullying, behaviour, and Safeguarding.

- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or Headteacher of any breaches of our policy.

Responding to an Online Safety Concern Flowchart

Content- is anything posted online
Conduct- means the way people behave online.
Contact- is about the risk of harm young people may face when interacting with other users online
Commerce- is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams

DSL – Charlotte Mulhall
DDSL – Nicky Olsen
LADO – 01522 554674



Online Safety Concern

Child

Inappropriate Content, Conduct, Contact or Commerce

Inform the **DSL**

Conduct or contact

Possible internal actions
- Sanctions (if deliberate)
- PSHE
- Restorative Justice
- Anti-bullying
- Parental work
- School support e.g. Counselling
- Request Support/ advice from Education Safeguarding tea

Content or Commerce

Report to internet and/or **filtering Service** Provider

(If illegal DSL will contact children's services who will advise on next steps which may be to report to, CEOP, Internet Watch Foundation www.iwf.ord.uk the police and/or social care as appropriate)

Staff (Visitors, volunteer, governors, supply teachers, contractors)

Illegal C,C,C,C

Report to **Headteacher** in line with allegations policy

(If concern relates to Headteacher in which case contact chair of Governors)

Report to **LADO/ Police**

If criminal or child protection investigation required report to, CEOP, Internet Watch Foundation www.iwf.ord.uk

Inappropriate Content, Conduct, Contact or Commerce

Report to **Headteache**r in line with allegations policy

(If concern relates to Headteacher in which case contact chair of Governors)

Report to internet and/or **filtering Service** Provider

(If illegal LADO will advise on next steps which may be to report to, CEOP, Internet Watch Foundation www.iwf.ord.ukthe police)

Possible internal actions
Advice received by LADO
- Staff training
- Disciplinary action if deliberate
- Internal support e.g. counselling
- Request support/ advice from Education Safeguarding Team

Record incident, action taken and decision -making in line with child protection recording systems (CPOMS). Review policies and procedures and implement changes.