CRADLEY CE PRIMARY SCHOOL

E Safety policy Autumn 2021

Policy developed by	R Homer
Reviewed	Autumn 2021
Approved by Governors	Spring 2022
Next review	Autumn 2024

Vision

Our aspirations for every child at Cradley CE are encapsulated in our vision statement: 'Believe, belong, be happy; every child, every chance, every day'. This, together with our core values of respect, belonging, caring, trust, forgiveness, resilience and perseverance drive all that we do.
Rationale

Rationale

'Safeguarding and promoting the welfare of children is ***everyone's*** *responsibility'* (KCSIE).

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools/academies are bound.

'It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.' (KCSIE September 2021)

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. At Cradley we want to equip pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. Cradley CE Primary School's Online safety/E-Safety policy helps ensure this safe and appropriate use.

New technologies are evolving constantly and being embraced by users. To reflect this, it is important that an Online safety/ e-safety policy is reviewed on a regular basis and children are taught the underpinning skills, knowledge and understanding that can help the children navigate the internet safely regardless of the device, platform or app.

Scope

This policy applies to all members of the school including: staff, pupils, volunteers, parents/ carers, visitors and community users who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of peer on peer abuse or other online safety/e-safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action will be taken as specified in our Behaviour Policy.

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

From September 2020, Relationships Education was compulsory for all primary aged pupils and Health Education was compulsory in all state-funded schools in England. Through these new

subjects, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers at Cradley C of E will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives. This will complement the computing curriculum, which covers the principles of online safety at all key stages.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk (known as the 4 C's):

- ***content:*** *being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.*
- ***contact:*** *being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*
- ***conduct:*** *personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying*
- ***commerce:*** *risks such as online gambling, inappropriate advertising, phishing and or financial scams*
  (KCSIE September 2021)

Development, Monitoring and Review of the Online safety/E-Safety Policy:

This Online safety/E-Safety policy has been developed by members of a working party consisting of:

- DSL/Headteacher
- Computing lead – E safety lead
- Safeguarding Governor

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Governors meetings

The school will monitor the impact of the policy using**:**

- Logs of reported incidents
- DGfL or internal monitoring logs of internet activity (including sites visited)
- Internal monitoring of data for network activity
- Surveys / questionnaires of stakeholders-including 'pupil voice'

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online safety/ E-Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety/online safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of Online safety/ E-Safety Governor- Mrs J Dunn – Governor responsible for safeguarding.

The role of the Online/E-Safety Governor will include:

- Regular meetings with the DSL
- Regular updates on the monitoring of Online safety/E-Safety incident logs
- Regular updates on the monitoring of the filtering of web sites/change control logs
- Reporting to relevant Governor meetings

Head teacher and Senior Leaders: Mrs M Harris and Miss Z Parkinson

The Head teacher is responsible for ensuring the safety (including Online safety /E-Safety) of members of the school community and is likely to be the school's Senior Information Risk Owner (SIRO). The school's SIRO is responsible for reporting security incidents as outlined in the schools Information Security Policy. The day to day responsibility for Online safety/ E-Safety will be delegated to the Deputy Headteacher and Computing Leader who has this responsibility.

- The Head teacher is responsible for ensuring a whole school approach to e-safety is taken by the school. They must create a culture that incorporates the principles of online safety across all elements of school life (policies and practices) and will proactively engage staff, parents and pupils in online safety.
- The Head teacher must embed the online safety principles in this document, modelling the online safety principles consistently and extending these to parents/carers.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal Online safety /E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
  (Guidance relating to the reporting procedure for* Online safety *E Safety incidents- see appendix 1. This should be viewed/amended/replaced in accordance with the current Child Protection/Safeguarding reporting procedures)

Safeguarding children procedures (dudley.gov.uk)

  The Head teacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious Online safety /E-Safety allegation being made against a member of staff

Management of Allegations- Allegations Against Staff (dudley.gov.uk)

- The Head teacher is responsible for ensuring that parents/carers understand that the school may investigate any reported misuse of systems, by pupils, out of school hours, as part of 'safeguarding' procedures.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online safety/E-Safety Coordinator: Mr R Homer

The school has a named person with the day to day responsibilities for Online safety/E-Safety.

Responsibilities include:

- Taking day to day responsibility for Online safety/E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies / Online safety documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online safety/E-Safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority Designated Officer (LADO) or relevant organisations
- Liaising with the school's SIRO to ensure all school data and information is kept safe and secure
- Receiving reports of Online safety/E-Safety incidents and creating a log of incidents to inform future E-Safety/Online safety developments
- Meeting regularly with the Online safety/E-Safety Governor to discuss current issues, review incident logs and filtering
- Attending relevant meetings / Governor committee meetings
- Reporting regularly to the Senior Leadership Team

Managed service provider:

The managed service provider is responsible for helping the school to ensure that it meets the Online safety/E-Safety technical requirements outlined by DGfL, which is aligned to national guidance. The managed service provides a number of tools to schools including e-Safe, Smoothwall filtering and MDMs (Mobile Device Management systems), which are designed to help schools/academies keep users safe -*(see appendix* 2).

Schools are able to configure many of these locally or can choose to keep standard settings.
A designated adult can access activity logs for network users and apply 'rules' to specific group of users. Schools should nominate a suitable member of staff to manage this responsibility and keep logs of any changes made to filtering and monitoring rules.
CC4 Anywhere and similar products, are applications that enables a user to remotely access documents and applications stored on the school server/servers. The school has responsibility for ensuring files and applications accessed via this system comply with information and data security practices.

The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Agreements/guidance *(see Appendix 3)* and include relevant Local Authority Online safety/E-Safety policies and guidance.
Safeguarding children procedures (dudley.gov.uk)
Online Safety and use of images (dudley.gov.uk)

Members of the DGfL team will support schools to improve their Online safety/E-Safety strategy. The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the DGfL team.

Teaching and Support Staff:

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face
In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. (KCSIE September 2021)

Staff are responsible for ensuring that:

- They have an up to date awareness of Online safety/E-Safety matters and of the current school Online safety/E-Safety policy and practices
- They have read and understood the most recent guidance specified in Teaching online safety in school-DfE (2019) and in Keeping children safe in education (2021)
- They encourage pupils to develop good habits when using IT to keep themselves safe
- They have read, understood and signed the school Staff Acceptable Use Agreements (AUA's)
- They report any suspected misuse or problem to the Online safety/E-Safety Co-ordinator for investigation.
- Digital communications with pupils (email / Virtual Learning Environment (VLE), applications/O365 Apps/Google Apps / voice) should be on a professional level and only carried out using official school systems
- Online safety/E-Safety issues are embedded in all aspects of the curriculum, in line with the statutory 2014 curriculum requirements
- Students / pupils understand and follow the school Online safety/E-Safety and acceptable use agreements
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are ware that the school has an acceptable use policy for staff, which encompasses all areas of digital technology and communication; such as, the use of mobile phones; photographing pupils; use of school cameras; downloading of photographs only on school computers; social media use (such as, Facebook, Twitter and other social media platforms) and understanding they should not invite children and young people, past or present pupils, onto personal social networking sites, internet use; email use (use of school email addresses only for children and young people's personal information) and encrypted or password protected memory sticks if transporting data.
- Teachers will enable pupils to identify possible online risks and make informed decisions about how to act. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.
- In lessons, where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. They include the teaching of Online safety/E-Safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies and the school will implement these sanctions in accordance with the AUA or any statements included in other policies.
- Teachers should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.
- Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

Designated person for Child Protection/ DSL

Mrs Marcia Harris is trained in Online safety/E-Safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Publishing of specific information relating to school based activities involving pupils, via official school systems such as the school web site, external school calendar, Twitter, Facebook, You Tube

- Sharing of school owned devices or personal devices that may be used both within and outside of the school
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying, Sexting and Sextortion, Revenge porn, Radicalisation, CSE

Students / pupils:

Students/pupils have access to the school/ network and technologies that enable them to communicate with others beyond the school environment. The network is a secure, monitored and safe system provided through DGfL. Students/pupils:

- Are responsible for using the school IT systems in accordance with the Student / Pupil Acceptable Use Agreement which is signed and in every child's planner.
- Need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to know how to spot techniques used for persuasion. This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.
- Need to be able to evaluate what they see online. This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites, video streaming facilities, digital image sharing sites and peer to peer abuse. This includes the implications of use outside of school
- Are responsible for the safe use of school owned equipment at home, in accordance with the school AUA, for these devices. The school AUA may be used.
- Should understand the importance of adopting good Online/E-Safety practice when using digital technologies out of school and realise that the school's Online/E-Safety policy covers their actions out of school, if related to the use of an externally available web based system, provided by the school
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.
- Should understand where to get help online and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. This will enable pupils understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website /workshops.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Agreement
- Promoting good online safety practice by following guidelines on the appropriate use of digital and video images taken at school events and their children's devices in school.

Community Users/ 'Guest Access':

Community Users who access school ICT systems will be expected to sign a Community User AUA before being provided with access to systems.

Policy Statement

Education – students / pupils

Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety, and recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed. Schools should consider all of this as part of providing a broad and balanced curriculum (colleges may cover relevant issues through tutorials). This may include covering relevant issues for schools through Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils in state-funded schools). (KCSIE September 2021)

There is a planned and progressive Online safety/E-Safety curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups. All staff have a responsibility to promote good Online/E-safety practices.
Online safety/E-Safety education is provided in the following ways:

- A planned Online safety/E-Safety/E-literacy programme is provided as part of Computing and is regularly revisited – this include the use of ICT and new technologies in and outside the school. Each year group begins the year with a unit dedicated to e-safety, this is then reinforced and embedded within other units across the year.
- Key Online safety/E-Safety messages are reinforced as part of a planned programme of assemblies.
- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy and plausibility of information
- Students / pupils are aware of the Student / Pupil AUA's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school
- Pupils are 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.
- Students/pupils are aware that their network activity is monitored and where students/pupils are allowed to freely search the internet their internet activity is being scrutinised
- Students/pupils may need to research topics that would normally be blocked and filtered. Any request to un-filter blocked sites for a period of time, must be auditable
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all rooms
- Students and pupils are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices
- Students are taught the consequence of their actions online and understand the age of criminal responsibility

Education – parents / carers

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

- Letters, newsletters and the school website
- Parents evenings
- Online/E-Safety sessions for parents/carers
- High profile events/campaigns e.g. Safer Internet Day

Education & Training – Staff

All staff receive regular Online safety/E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal Online safety/E-Safety training is made available to staff. An audit of the Online safety/ E-Safety training needs of all staff is carried out regularly. It is expected that some staff will identify Online safety/E-Safety as a training need within the performance management process
- All new staff receive Online safety/E-Safety training as part of their induction programme, ensuring that they fully understand the school Online safety/E-Safety Policy and Acceptable Use Agreements
- The Online safety/E-Safety Coordinator/DSL receives regular updates through attendance at DGfL training sessions and by reviewing guidance documents released by DfE / DGfL / LA, LSGB and others
- This Online safety/E-Safety policy and its updates are presented to and discussed by staff in staff meetings.
- The Online safety/E-Safety Coordinator/ DSL provides advice / guidance / training as required to individuals
- All staff are updated of new guidance as and when it occurs

All staff are familiar with the school policy including:

- Safe use of e-mail
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other school approved system
- Safe use of the school network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs/videos/posts/blogs/calendars and information available on the school website and twitter feed
- Capturing and storing photographs/videos/audio files on personal and school owned devices
- Cyberbullying procedures
- Their role in providing Online safety/E-Safety education for pupils
- The need to keep personal information secure
- Safe and appropriate use of social media

All staff are reminded / updated about Online/E-Safety matters at least once a year.

Training – Governors

Governors/Directors take part in Online safety/E-Safety training / awareness sessions, particularly those who are members of any sub-committee / group involved in ICT/Computing / Online safety/E-Safety / Health and Safety / Child Protection

.

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL/ LSGB or other relevant organisation
- Participation in school training / information sessions for staff or parents

- Invitation to attend lessons, assemblies and focus days

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school 'managed' infrastructure / network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this document are implemented.

Filtering
DGfL filtering is provided by Smoothwall. The IWF (Internet Watch Foundation) list and the "police assessed list of unlawful terrorist content, produced on behalf of the Home Office", is integrated into the Smoothwall database.
Web filtering policies are applied based on:
"who" (user or user group from a directory),
"what" (type of content),
"where" (client address – either host, subnet or range),
"when" (time period) in a filtering policy table that is processed from top-down

Monitoring
DGfL's monitoring solution is provided by e-Safe. e-Safe's detection technology monitors imagery, words and contextual phrases, during online and offline activity, to identify behaviour which may represent a safeguarding risk or breach of acceptable use policies.

School ICT systems will be managed in ways that ensure that the school meets the Online/E-Safety technical requirements outlined in the AUA's

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted to authorised users

All users will have clearly defined access rights to school ICT systems

- All users will be provided with a username and password
- Users will be required to change their password every few months
- Users will be made responsible for the security of their username and password. They must not allow other users 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
- The school's password system means that passwords must be at least 10 characters long, including upper and lower case letters, numbers and special characters. They will be locked out of their account after 8 attempts and will not be able to use a password similar to one they have previously had.
- The school maintains and supports the managed filtering service provided by DGfL. The school can provide enhanced user-level filtering through the use of Smoothwall filtering
- The school manages and updates filtering issues through the RM Service desk
- Requests from staff for sites to be removed from the filtered list will be considered by Mrs M Harris or Mr R Homer (IT lead). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online safety/E-Safety Committee.
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual / potential Online safety/E-Safety incident to the relevant person
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc

from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place for the provision of temporary access to "guests" (e.g. trainee teachers, visitors) onto the school system. This is auditable
- A guardianship document is signed before school owned equipment leaves the premises. This clearly outlines the user's responsibilities.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured
- The school has responsibility for ensuring files and applications accessed via CC4 Anywhere or a similar application, comply with information and data security practices.

Curriculum

Online/E-Safety is a focus in all areas of the curriculum. The new Computing Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy is taught. Staff will re-enforce online safety/E-Safety messages in the use of ICT across the curriculum and during Computing lessons.

- In lessons, where internet use is pre-planned, students / pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about Online/E-Safety
- The school teaches 'Digital Literacy' as part of the new 'Computing' programme of study
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Use of digital and video images

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, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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

- Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the storing, sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and comply with good practice guidance on the use of such images
- Students' / pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of students / pupils are published on the school website or twitter feed
- Student's / pupil's work can only be published with the permission of the student / pupil and parents or carers. Parents should have signed the DSCB consent form
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Data Protection

The school has a Data Protection Policy that meets statutory guidance.

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff are aware of the 'School Information Security Policy'. A breach of the Data Protection Act may result in the school or an individual fine of up to £500000

Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- Access personal data on secure password protected computers, 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

When personal data is stored on any portable computer system, USB stick or any other 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.

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. Staff and students / pupils should therefore use only the school email service to communicate with others when in the school, or on school systems e.g. by remote access from home
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students / pupils or parents / carers (email, chat, school 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 public chat / social networking programmes must not be used for these communications
- Older students / pupils are provided with individual school email addresses for educational use
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website, on public facing calendars and only official email addresses should be used to identify members of staff
- Mobile phones may be used by children in year 5 and 6 when they walk to school on their own. The must not be brought into school but switched off and handed into the school office before school starts. They will then be handed back at the end of the day.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school. Phones and other devices are stored in lockers in the staff room. They are never to be brought in the classroom with the children.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school has a policy that sets out clear guidance for staff to manage risk and behaviour online.

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
- 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 students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff are not allowed parents as friends.

When using official school social media accounts, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff- to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.
- A school based code of behaviour for users of the accounts, including: Systems for reporting and dealing with abuse and misuse, Understanding of how incidents may be dealt with under school disciplinary procedure

We encourage the safe and responsible use of social media through using sites such as Facebook, Twitter, etc. These sites can be used to share information and news that can be rumours, and unverified stories that could cause worry within communities. Below are some tips that you can use to help protect you online.

The Do's

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the employer's logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

The Don'ts

- Don't make comments, post content or link to materials that will bring your employer into disrepute

- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of the content you share, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
The school will take all reasonable precautions to ensure Online safety/E-Safety is a key focus. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by tutor / Head of Year / E-Safety/Online safety Coordinator / Head teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to LA SPA

Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

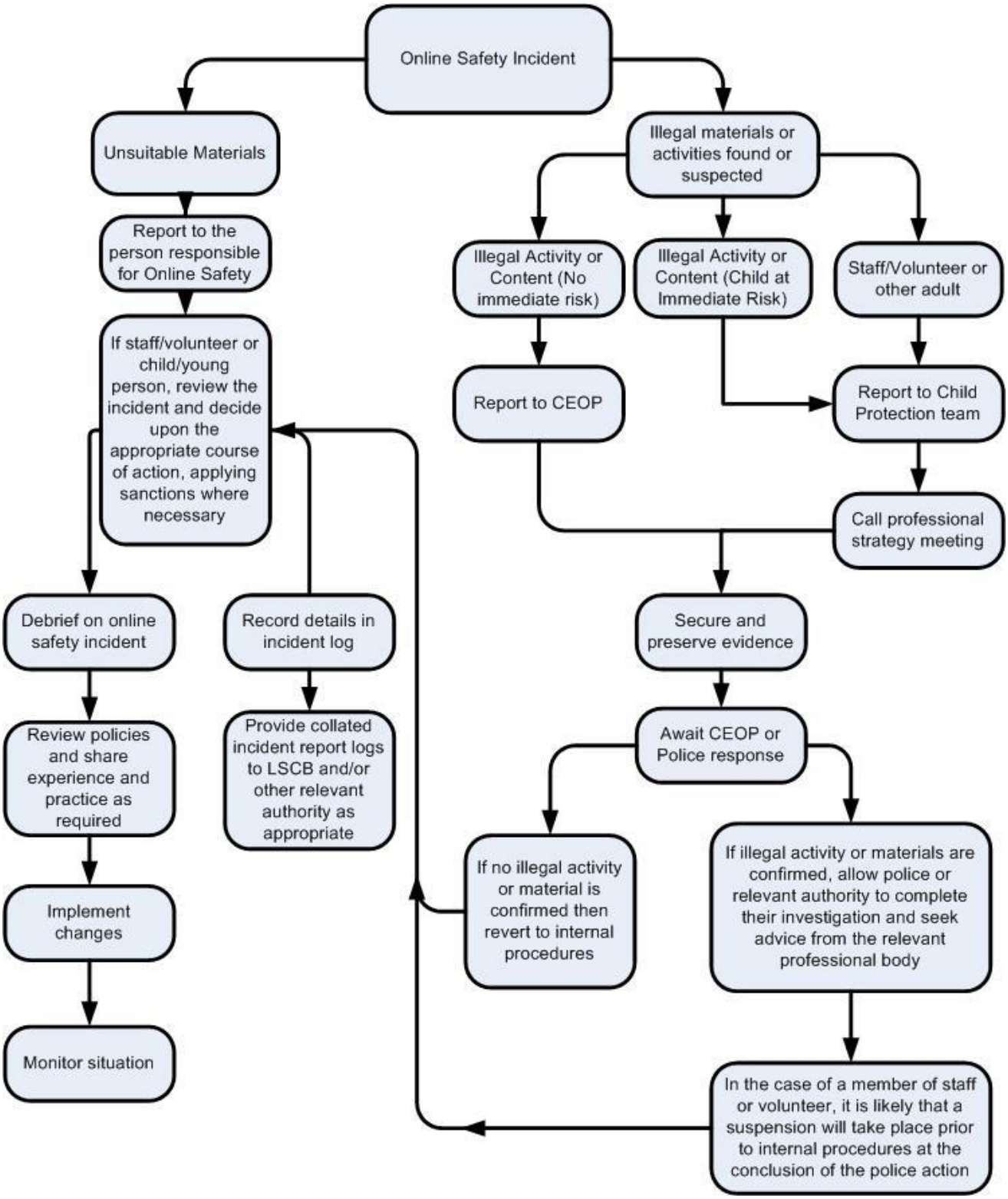
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school, LSGB child protection procedures.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

This E-Safety Guidance and Policy has been written with references to the following sources of information:

Dudley LA
Hertfordshire E-Safety Policy
Kent e-Safety Policies, Information and Guidance
South West Grid For Learning- Online Safety School template Policies

Appendix 1 - E-Safety/Online safety sample response



Appendix 2-E-Safety/Online safety tools available on the DGfL network

E-Safety tool	**Type**	**Availability**	**Where**	**Details**
Smoothwall filtering	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUA	Awareness raising	Part of CC4-needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
eSafe	Monitoring software-*licenses available on Windows, Apple Mac*	Available to all schools	All school Windows 7 or 8.1 desktops and networked laptops and Apple Mac networks	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored. Reports are sent to designated staff in school
Email	Filtering and list control	Provided as part of DGfL	Office 365	Allows schools to restrict where email is sent from/to
RM Password Plus	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management tool that enforces password rules of complexity and length for different users