GRAYSWOOD PRIMARY SCHOOL
Church of England (Aided)

Online Safety Policy

Policy Schedule	
Last reviewed:	Autumn 2025
Next review:	Autumn 2026

Version history- version 2 - the following was adapted/added/changed on 3/10/2023

Section	Changes made	By whom
Contents Page 3	Contents page added	Hannah Cole
Legislation and Guidance Page 4	'…given teachers stronger powers to tackle cyber-bullying by examining and deleting any images or files on pupils' electronic devices where they believe there is a 'good reason' to do so' changed to '…given authorised school staff stronger powers to tackle cyber-bullying by examining any data or files on an electronic device that they have confiscated, if they have good reason to do so.'	Richard Stanton
Roles and responsibilities Page 5	'It is the responsibility of the ICT manager…' changed to 'It is the responsibility of the DSL team and ICT Manager'	Richard Stanton
Acceptable use of email Page 9	Section on 2 Factor Authentication (2FA) added	Richard Stanton
Filtering and Monitoring Page 11	Section on filtering and monitoring added in light of new guidance in Keeping Children Safe in Education	Richard Stanton
Parental Involvement Page 13	'…the online safety page of the school website' added to 'e.g. class Friday Notes, updates on whole-school newsletters, the online safety page of the school website and parent workshops where appropriate.'	Richard Stanton
Secure storage and access to data Page 14	'When personal data is stored on any portable computer system, USB stick or other removable media:' changed to 'when personal pupil data e.g, class information, assessment scores/levels and pupil reports is stored on any portable computer system, USB stick or other removable media'.	Richard Stanton

The following was adapted/added/changed on 17/11/2024

Section	Changes made	By whom
Online Safety Page 12	'The updated definition of safeguarding in KCSiE 2024 part one, now explicitly includes recognition that children may be maltreated online – 'Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as…protecting children from maltreatment, whether that is within or outside the home, including online'.'	Richard Stanton

The following was adapted/added/changed on 25/9/2025

Section	Changes made	By whom
The 4 Key categories of risk Page 4	**'Content'** category updated to included KCSiE 2025 terms 'misinformation, disinformation (including fake news) and conspiracy theories'	Richard Stanton
Legislation and Guidance Page 4	A link to the 'Online Safety Act: Explainer' has been added to the list of Gov/DfE guidance which this policy refers to.	Richard Stanton
Misinformation, disinformation and conspiracy theories Page 13	Subsection '10.2 Misinformation, disinformation and conspiracy theories' added to 'Section 10 Online Safety'	Richard Stanton
Artificial Intelligence (AI) Page 13	Subsection '10.3 Artificial Intelligence (AI)' added to 'Section 10 Online Safety'	Richard Stanton
Secure storage and access to data Page 15	'Personal data can only be accessed on machines that are securely password protected' extended to include 'or require 2 Factor Authentication (2FA) to gain access.'	Richard Stanton

Contents

1. Introduction

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used in supporting learning without creating unnecessary risk to users. It is also intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018.

2. Aims

Through implementation of this policy, Grayswood CE Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalization, extremism, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- Online Safety Act

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Searching, Screening and Confiscation Guidance, July 2022, which has given authorised members of school staff stronger powers to tackle cyber-bullying by examining any data or files on an electronic device that they have confiscated, if they have good reason to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

It is the responsibility of Governors, The Headteacher, ICT Manager and Computing Co-ordinator that this policy is properly implemented.

It is the responsibility of all staff to ensure that this policy is adhered to and that learners are not placed at unnecessary risk. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

In addition, staff working with learners using communications equipment ensure that learners are aware of the appropriate rules and that these rules are adhered to. If this policy is breached for any reason, it is the responsibility of the members of staff to inform the Headteacher as soon as they are able.

The DSL team and ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

5. Acceptable Use of the Internet

5.1 Internet use

Grayswood CE Primary School expects all users to use the Internet responsibly and strictly according to the following conditions.

Users do not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography of any kind

- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to others

Incidents which appear to involve deliberate access to web sites, newsgroups and online groups that contain the following material may constitute gross misconduct leading to summary dismissal and/or be reported to the police:

- Images of child abuse (images of children, under 16 years old) involved in sexual activity or posed to be sexually provocative
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK

In addition to the above, users must also ensure that they do not:

- Use the facilities at or belonging to Grayswood CE Primary School for running a private business
- Enter into any personal transaction that involves the school or Surrey County Council in any way
- Visit sites that might be defamatory or incur liability on the part of Grayswood CE Primary School or Surrey County Council or adversely impact on the image of Grayswood CE Primary School or Surrey County Council
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information
    - personal information
    - databases and the information contained therein
    - computer\network access codes or passwords
    - business relationships

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses\malicious software and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate

5.2 Issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

5.3 Personal Use

Staff are permitted to access the Internet for personal use on a limited basis with the approval of their line management as long as this does not interfere with their job responsibilities. This should be in own time or if being used for Teaching and Learning purposes. Learners are permitted access to the Internet for personal use if it is supervised and there is a reasonable justification for supporting their learning and\or developing their skills.

5.4 Respecting copyright

Users with Internet access must comply with the copyright laws of all countries relevant to education services. Users must not intentionally download any material that holds a copyright notice. This also relates to downloading and copying unlicensed software.

Virus and malicious software protection

Although virus protection software is installed on all networked computers, users should be aware of the potential hazards associated with computer viruses and malicious software. Any files that are downloaded will be scanned for viruses before being accessed. If you have any concerns about viruses\malicious software or think you may have accessed material that contains such, stop using the equipment and contact the Computing Co-ordinator or IT Technician as soon as possible.

5.5 Security

Staff are aware of the potential risks associated with accessing the Internet. Staff should be aware that newsgroups\user groups\social networking sites such as Instagram and Facebook are public forums where it may be inappropriate to reveal confidential or personal information. There is a need to be responsible, respectful and above all, professional:

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for school or Surrey County Council and your personal interests
- You must not engage in activities involving social media which might bring Grayswood CE Primary School or Surrey County Council into disrepute
- You must not represent your personal views as those of Grayswood CE Primary School or Surrey County Council on any social medium
- You must not discuss personal information about pupils, Grayswood CE Primary School or Surrey County Council staff and other professionals you interact with as part of your job on social media
- You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, Grayswood CE Primary School or Surrey County Council

- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Grayswood CE Primary School or Surrey County Council

5.6 Personal use of social media

- Staff members must not identify themselves as employees of Grayswood CE Primary School or Surrey County Council or service providers for the school or Surrey County Council in their personal webspace. This is to prevent information on these sites from being linked with the school and the Surrey County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services
- Staff members must not have contact through any personal social medium with any pupil, whether from Grayswood CE Primary School or any other school, unless the pupils are family members
- Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity
- Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, Surrey County Council staff and other parties and school or Surrey County Council corporate information must not be discussed on their personal webspace
- Photographs, videos or any other types of images of pupils and their families or images depicting staff members wearing school or Surrey County Council uniforms or clothing with school or Surrey County Council logos or images identifying sensitive school or Surrey County Council premises must not be published on personal webspace
- School or Surrey County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media
- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself
- Grayswood CE Primary School or Surrey County Council corporate, service or team logos or brands must not be used or published on personal webspace
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. Personal views and opinions about any subject should be carefully moderated by staff before they post on social media

sites. Language that is used should also be carefully considered by users social media sites so as not to cause offence or insult to others

6. Acceptable use of email

Each member of staff is given an e-mail account if their job responsibilities require such. Otherwise, one can be requested at the discretion of the Headteacher through line management. Teaching staff are expected to check emails on a daily basis and respond timey where required.

Teachers will also have access to a class email address and it is this which should be used when corresponding with parents directly, rather than their personal work account.

- When an email from a parent is received, teachers will respond by the end of the next working day, unless circumstances deem this unfeasible e.g while away on a class residential
- When emailing a parent, children's initials should be used, not full names and information about a child should only be shared with the parents/carers of that individual
- The content of emails should not be shared with any other staff member unless it is necessary to do so, e.g. sharing with a class TA/LSA or making the DSL aware of a safeguarding disclosure

At times, emails will be sent and received before or after teaching hours. Whilst teachers may respond to these if they wish to, there is no obligation for them to do so outside of recognised working hours (8am-5pm), nor should this be an expectation of them. There is a mutual understanding that teachers will respond to emails from colleagues or parents at the earliest opportunity and within 2 days.

6.1 Personal Use

Staff are permitted to send personal e-mails on a limited basis as long as this does not interfere with their job responsibilities.

6.2 Confidentiality

Messages sent and received via the Internet are regarded as having the same legal status as a corporate letter. Any material that is viewed as highly confidential or valuable to Grayswood CE Primary School should not be e-mailed externally.

6.3 Inappropriate behaviour

Users must not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations. Messages must not contain material or language that could be viewed as offensive to others or as contravening the school's Equal Opportunities Policy, N.B. what may appear appropriate to one person might be misconstrued by another.

6.4 Virus Protection\Malicious software

To prevent the risk of potential viruses\malicious software, users should not open any unsolicited e-mail attachments or independently load any software, including screensavers, onto their information and communications equipment.

6.5 Security
E-mail is an effective way of communicating information. This is only the case, however, if passwords are secure. To maintain security, it is good practice for users to change their passwords regularly. E-mail should not be left running unattended in any circumstances where this may lead to unauthorised access. The system should be closed and re-opened on return. In no instances will a user login using a colleague's password unless permission has been given from line management.

6.6 2 Factor Authentication
To further enhance security when using e-mail, two-factor authentication (2FA) is in place for all staff. To access their school email account, users are required to enter their self-generated password, along with a one-off code sent to their personal mobile phone.

7. Staff Laptop and ICT Equipment Loans
Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this online safety Policy. This must be the case wherever the laptop, computer or other such device is being used as it remains the property of Grayswood Primary School at all times. Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense. All staff members will take appropriate steps to ensure their devices remain secure. This may include, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

8. Acceptable use of Mobile Phones
Children are not allowed to bring mobile telephones into school, unless agreed by the Headteacher. If, on any occasion they are brought in, they are handed into the school office and locked away, being returned to the pupil's parent/carer at the end of the day. Grayswood Primary School will endeavour to keep any property left at reception safe but will not accept any liability for property left by the children howsoever caused.

Staff educate learners that E-Safety considerations also apply to mobile phones and computer devices they may use at home. Staff and other adults in the school should not use the cameras on their mobile phones to take photographs of the children. On the rare occasion that this is necessary, any image taken of children should be uploaded securely at school to the relevant storage file and then the images deleted from the user's mobile phone. During whole-school festivals and plays, parents

and carers are advised that photos or videos they take on their phones or tablet devices should only be of their own child/ren and be seen only by themselves.

8.1 Personal Mobiles – Staff

- Staff are not permitted to make/receive calls/texts during contact time with children
- Staff should have their phones on silent or switched off and out of sight (eg in a drawer, handbag) during class time
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground)
- Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g in office areas, staff room, empty classrooms
- Staff must security protect access to their phone
- Should there be exceptional circumstances (e.g acutely sick relative), then staff should make the Headteacher and office staff aware of this so that messages can be relayed promptly
- Staff should report any usage of mobile devices that causes them concern to the Headteacher

8.2 Mobile Phones for work related purposes

- We recognise that mobile phones provide a useful means of communication on off-site activities. During such times, staff should ensure that:
- Mobile use on these occasions is appropriate and professional
- Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the School Office
- Where parents are accompanying trips, they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children
- Mobile phones should not be used to take photos of students or staff while on the trip
- Where a mobile phone has school email accounts installed on the device the phone MUST be secured with a suitable pin, fingerprint id, facial recognition and encrypted to prevent unauthorised access
- Mobile devices using school email accounts should use the outlook app and not the devices built in mail client

8.3 Parents

While we would prefer parents not to use their mobile phones while on school premises, we recognise that many parents see their phones as essential means of communication at all times. We therefore ask that parents' usage of mobile phones, whilst on the school site is courteous and appropriate to the school environment. We do allow parents to photograph or video school events such as shows or sports day using their mobile phones – but insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own. Parents/carers are reminded of this at the start of every school performance, on sports day, etc and will receive written reminder in school newsletters as necessary.

9. Filtering and Monitoring

Keeping Children Safe in Education states that all schools should have appropriate and robust filtering and monitoring systems in place. The usage of all computers (and portable memory devices)

belonging to Grayswood CE Primary School or connected to Grayswood CE Primary School's network are monitored and all users have to agree to this in order to access the network.

9.1 What is filtering and monitoring?
Filtering systems block access to harmful websites and content.

Monitoring systems:

- Identify when someone searches for or accesses certain types of harmful online content on school devices
- Identify who is searching for or accessing the harmful content
- Alerts the school about it so we can intervene and respond
- **Don't** block access to harmful content

No software is perfect and reasons why filtering and monitoring software may not detect certain things are:

- It might not be aware of all the websites that contain inappropriate content
- Abbreviations or misspellings in a search engine may slip past the software
- Inappropriate content may be found on websites considered 'safe'

9.2 Who is responsible for filtering and monitoring?
Everyone at Grayswood CE Primary School has the responsibility of making sure children are using devices appropriately and can do this by:

- Monitoring what pupils are accessing on devices during school hours (e.g. by looking at their screens when using computers during lessons)
- Alerting one of our DSLs if you become aware that content is not being filtered

If you have concerns about what a pupil is accessing online, always raise it with a DSL.
Inappropriate content includes:

- Illegal content (e.g. child sexual abuse)
- Discriminatory content (e.g. sexist, racist or homophobic content)
- Sites that promote drugs or substance abuse
- Extremist content (e.g. the promotion of terrorism)
- Gambling sites
- Malware and/or hacking software
- Pornography
- Pirated material (copyright theft)
- Sites that promote self-harm, suicide and/or eating disorders
- Violent material

9.3 What systems do we use at Grayswood?
We have the following systems in place:

- Netsweeper – this is the name of the filtering platform we use. Netsweeper meets the government requirements for filtering and are part of the Internet Watch Foundation

- Netsweeper records every search term used. It will automatically block harmful content, including threats against online bullying, radicalisation and terrorist organisations, child sexual exploitation, drug abuse, self-harm and fake news
- Netsweeper functions across every device from desktops and tablets to smart phones.
- The DSL and IT Technician, William England, are responsible for monitoring and reviewing the filtering system regularly at DSL meetings
- DSLs and William receive daily reports of all searches and words used.
- Any concerns are followed up immediately and an internal investigation will take place by the DSL team
- The DSL Team will review monitoring and filtering reports at least once every half term and implement any changes needed
- We have also recently implemented 2 factor authentication on all email accounts to protect against cyber attacks. Staff are required to use 2 Factor authentication on all devices at school, including smart phones.
- If staff are suspicious of any email they do not open it but contact William for further advice and support.

The school filtering and monitoring systems are in place to prevent or limit access to sites in the spirit of this policy and to avoid any unnecessary risk to learners and staff. It is designed to protect pupils and staff online and should not have an impact on teaching and learning or school administration.

In the event that pupils or staff cannot access content they need to carry out their work or have access to content that should be blocked, the Headteacher, Hannah Cole and DSL must be notified and she will then speak to William about whether to allow access. A written record of requests will be kept.

10. Online safety

As online safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Computing Co-ordinator and DSL to keep abreast of current issues and guidance through organisations such as Ofsted, CEOP (Child Exploitation and Online Protection) and Childnet. The updated definition of safeguarding in KCSiE part one, now explicitly includes recognition that children may be maltreated online – 'Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as…protecting children from maltreatment, whether that is within or outside the home, including online'.

Online safety should therefore be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum and as such we provide opportunities within the ICT and PSHE curriculum areas to teach about online safety, which include:

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum
- Teaching about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the ICT curriculum

- Making pupils aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies (see below - cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

In lessons where internet use is pre-planned, it is best practice that 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. Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Grayswood CE Primary School takes all reasonable precautions to ensure that users access only appropriate material
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Staff ensure that learners are encouraged to enjoy the safe use of digital technology and to use ICT to enrich their learning. Learners are made aware of risks and processes for safe digital use
- All staff using information and communications equipment residing in, and\or belonging to Grayswood CE Primary School are given time and training to understand this policy and are expected to read it and implement it into their practice.
- Learners are taught to evaluate digital materials appropriately and are given age-appropriate rules in which to follow. If inappropriate material is viewed by children unintentionally, they must immediately close the computer/device and inform a teacher, who in turn will inform the Headteacher
- Teaching staff educate pupils in the effective use of the Internet in research including the skills of knowledge location, retrieval and evaluation. They educate pupils in the recognition of bias, unreliability and validity of sources and actively educate learners to respect copyright law
- Staff, Governors, Parents and carers are made aware of this policy
- Parents and carers are discouraged from allowing computer equipment to be placed in children's bedrooms and that children are supervised at all times when accessing information and communications equipment
- Staff only use individual pupil images or computer-based work in a way that will not enable individual pupils to be identified and, if used externally, when approved by parents or carers
- Staff also ensure that when used, webcams and\or video conferencing use is always supervised appropriately

10.1 Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We strive to work in partnership with parents/carers and to discuss online safety wherever possible and seek to promote a wide understanding of the benefits related to ICT and potential risks. Parents/carers are required to decide as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website) and the school disseminates information to parents relating to online safety where appropriate in a variety of forms e.g. class Friday Notes, updates on whole-school newsletters, the online safety page of the school website and parent workshops where appropriate.

10.2 Misinformation, disinformation and conspiracy theories

Disinformation, misinformation and conspiracy theories are online safety risks for children. They refer to the spread of false information or 'fake news' online and mean that children can be more at risk of taking this content at face value. Advanced AI tools can be used to present the information as fact, making it appear realistic, including the use of AI-generated images and videos. As school staff we all have a role to play to ensure pupils are kept safe online from this risk and that opportunities are taken to make children aware of them and know how to keep themselves safe.

10.3 Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Copilot and Google Gemini. At Grayswood CE Primary School we use Microsoft Copilot.

Grayswood CE Primary School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by Grayswood CE Primary School and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

11. Cyberbullying

Cyberbullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology. It can take many forms but can go even further than face to face bullying by invading home and personal space and can target one or more people. It can take place across age groups and target pupils, staff and others and include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.

Cyberbullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages;
- Threatening or embarrassing pictures and video clips via mobile phone cameras;

- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- Menacing or upsetting responses to someone in a chat-room;
- Unpleasant messages sent during instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook)Text / video messaging

Grayswood CE Primary School works to prevent cyberbullying in the following ways:

- The DSL will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying;
- Staff will be trained to identify signs of cyberbullying and will be helped to keep informed about the technologies that children commonly use;
- Pupils will be informed about cyberbullying through curricular and pastoral activities and an annual Online safety Week. During this week, parents will be provided with information and advice on cyberbullying;
- Positive use of ICT will be promoted across all year groups, and will be kept up to date as technologies develop;
- CPD and INSET may be used to help staff develop their own practices and support pupils in safe and responsible use of ICT;
- The school will encourage safe use of ICT, emphasising, for example, the importance of password security and the need to log out of accounts.

The school will promote the message that asking for help is the right thing to do and all members of the school community will be informed how cyberbullying can be reported. Confidential records will be kept of all cyberbullying incidents. A cyberbullying incident might include features different to other forms of bullying, prompting a particular response. Further details can be found in the school's anti-bullying policy.

12. Secure storage and access to data

The school will ensure that ICT systems are set up so that protected files are hidden from unauthorised users and that users will determine which files are accessible to them. Personal data can only be accessed on machines that are securely password protected or require 2 Factor Authentication (2FA) to gain access. Any device that can be used to access data must be locked if left unattended, even if only for very short periods.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. Personal data can only be stored on school equipment, including staff laptops, though remote access to the shared drive means this should not be necessary. When personal pupil data e.g, class information, assessment scores/levels and pupil reports is stored on any portable computer system, USB stick or other removable media:

- The data must be encrypted and password protected

- The data must be securely deleted from the device once it has been transferred or its use is complete
- If your device is set to backup to cloud locations it should also be deleted from there too

13. Secure transfer of data and access outside of school

The school recognises that personal data may be accessed by users out of school, or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorise premises without permission from the Headteacher and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the school's network
- Users must protect with approved encryption software all portable and mobile devices, including media, used to store and transmit personal information
- Users must be aware that printing documents remotely can also lead to breach in data protection and should only print documents when at school

14. Equal Opportunities - Pupils with Additional Needs

Our school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well-managed for these children and young people.

15. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL/DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, when and if applicable.

16. Linked Policies

For further information, the following policies can be referred to:

- Anti-Bullying
- Behaviour
- EYFS
- Equality
- Expectations for Remote Learning
- Safeguarding and Child Protection Policy
- Staff Code of Conduct