

THE GROVE PRIMARY SCHOOL



Online Safety Policy

5.0

Status:	Current	
Date Adopted by Governing body:		
Review Date:	September 2023	Yearly
Created by:		
Rebecca Denmeade	March 2018	1.0
	January 2021	2.0
	January 2022	3.0

	October 2022	4.0
	July 2023	5.0
Reviewed by Full Governing Body and Online Safety Committee	October 2022	4.0
	September 2023	5.0

This policy should be read and understood in conjunction with the following documents:

- **General Consent Form**
- **Behaviour and Conduct Policy**
- **Anti- Bullying Policy**
- **Child Protection Policy**
- **Data Protection Policy**
- **Mobile Phone Policy**
- **Remote Learning Policy**
- **Social Networking Policy**
- **Code of Conduct for Staff, Governors and Volunteers**
- [Guidance for Safer Working Practice for Adults working with Children and Young People \(February 2022\)](#)
- [Keeping Children Safe in Education \(DfE\)](#)
- [Screening, Searching and Confiscation at schools \(DfE 09/22\)](#)
- [Education for a Connected World framework \(UK Council for Internet Safety 2020 Edition\)](#)
- [Teaching online safety in schools \(DfE Published January 2023\)](#)
- [Teachers' Professional Standards \(DfE Updated December 2021\)](#)
- [SWGfL Project Evolve – online safety curriculum programme and resources](#)

APPENDICES:	
A	Staff and Volunteer Acceptable Use Agreement
B	Parent Acceptable Use Agreement
C	General Consent Form (KS1)
D	General Consent Form (KS1)
E	Online Safety Incident Flow chart
F	Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart)
G	Technical security

8	Filtering and monitoring procedures
9	Form to request temporary removal of filtering

Contents

1. Aims.....	3
2. Legislation and guidance.....	4
3. Roles and responsibilities.....	5
4. Educating pupils about online safety.....	11
5. Educating parents about online safety	13
6. Cyber-bullying.....	14
7. Acceptable use of the internet in school	15
8. Pupils using mobile devices in school.....	20
9. Staff using work devices outside school	20
10. How the school will respond to issues of misuse	21
11. Training.....	21
12. Monitoring arrangements	22
13. Links with other policies	23

1. Scope of the policy

- This policy applies to all members of the school community (including staff, pupils, governors, volunteers, and visitors) who have access to and are users of school's digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site where allowed.
- The Education and Inspections Act 2006 empowers head teachers 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 cyber-bullying or other online 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](#) and [The Schools \(Specification and Disposal of Articles\) Regulations 2012](#) increased these powers with regard to the searching for and of electronic devices and the deletion of data as did well as the guidance from the DfE entitled [Screening, Searching and Confiscation at schools \(DfE 09/22\)](#)

- The school will deal with such incidents within this policy and associated policies as referenced above and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

2. Aims

Our 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
- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world

The 4 key categories of risk

Our approach to teach, manage and monitor 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, anti-Semitism, radicalisation and extremism
- **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, sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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](#)
- [Relationships and sex education](#)

› [Searching, screening and confiscation](#)

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 [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

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

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and/or parents online have a responsibility to model safe practice at all times.

In addition to the roles and responsibilities outlined below, and to support the implementation of this policy, the school has compiled 'Acceptable Use Agreements' (AUAs), which provide clear guidance in relevant areas such as conduct, access to and use of the school system, removable media, downloading files, sharing information, social networks and devices (both school and personal equipment within and outside school).

- Separate agreements have been written for:
 - staff and volunteers
 - governors
 - pupils
 - parents

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing body will attend regular meetings, as part of it's Safeguarding Committee, with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). These meetings will be organised by the Online Safety Coordinator- Rebecca Denmeade- and will be attended by the following key stakeholders for Online Safety:

- Online Safety Governor, Chair of Governors
- Head teacher, DSL
- Online Safety Coordinator
- Deputy Head

- SENDCo
- Computing Coordinator
- Computing TA

The governor who oversees online safety is the Chair of Governors

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The head teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The head teacher will also be present at all Online Safety Group meetings to discuss Online Safety, review and monitor online safety incidents and logs.

- The head teacher has a duty of care for ensuring the safety (including online safety) of members' of the school community and fostering a culture of safeguarding, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator (OSC).
- The head teacher and all members of the senior management team (SLT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (Appendix F – 'Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart)' and relevant Local Authority disciplinary procedures.
- The head teacher and SLT are responsible for ensuring that the OSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The head teacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The head teacher and SLT will receive regular monitoring reports from the OSL- a report on any incidents and necessary follow up actions will be provided by the OSL at each Safeguarding Committee Meeting.

3.3 The designated safeguarding lead

Details of the school's DSL and DDSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DDSL takes lead responsibility for online safety in school (due to the head teacher being the DSL), in particular:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy including accurate reporting and recording using either CPOMs
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head teacher and/or governing body

This list is not intended to be exhaustive.

3.4 The Online Safety Coordinator

The OSC will be a member of the SLT and their responsibilities are to:

- lead the Online Safety meeting with relevant stake holders:
 - Online Safety Governor, Chair of Governors
 - Head teacher, DSL
 - Online Safety Coordinator
 - Deputy Head
 - SENDCo
 - Computing Coordinator
 - Computing TA
- work closely on a day to day basis with the DSL where these roles are not combined
- take day to day responsibility for online safety, being aware of the potential for serious child protection concerns
- have a leading role in reviewing the school's online safety policy, procedures and documents
- promote an awareness and commitment to online safety education/awareness, raising concerns across the school and beyond
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (i.e. misuse – see Appendix F)
- provide (or identify sources of) training and advice for staff, governors, parents and pupils
- be aware of external sources of support and guidance in dealing with online safety issues (e.g. local authority, police etc) and liaise with the Local Authority (LA) and other external agencies as relevant
- liaise with the school's technical support and external providers
- receive and log online safety incidents to inform practice, policy review and development
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and, if possible filtering and monitoring logs

- attend relevant meetings
- report regularly to the SLT
- review emerging technologies for educational benefit and carry out a risk assessment before use in school is allowed.

3.5 The ICT manager

The 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and reported to the Online Safety Coordinator.

The ICT manager is responsible for ensuring that:

- they are aware of and follow the school's Online Safety Policy and Technical Security Procedures to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority
- there is clear, safe and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the OSL and wider Safeguarding Team (where necessary) for investigation and action
- the filtering procedures are applied and updated on a regular basis and their implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in school policies
- This list is not intended to be exhaustive.

3.6 Computing curriculum lead

- Curriculum Leads will work with the OSC to develop a planned and coordinated online safety programme (e.g. [National Online Safety](#)), with reference to the DfE guidance: [‘Teaching online safety in schools’ \(January 2023\)](#).
- This will be provided through:
 - a discrete programme- the school currently uses the learning structure and resources provided by the National Online Safety Platform
 - PHSE and RHE/SRHE programmes
 - assemblies and pastoral programmes
 - through relevant initiatives and opportunities (e.g. Safer Internet Day and Anti-Bullying Week)

3.7 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet, and ensuring that pupils follow the school’s terms on acceptable use
- Working with the DDSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with promptly and appropriately in line with the school’s behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet
- Parents are responsible for using the school’s digital technology systems in accordance with the ‘Parents’ AUA’ which they are required to read and sign when their child joins the school.
- Parents play a crucial role in ensuring that their children understand the need to use internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:
 - publishing the school Online Safety Policy on the website
 - parents’ evenings
 - newsletters and letters
 - the school’s website and learning platform
 - information about national and local online safety campaigns

- free access to the parental portal on the National Online Safety platform
- Parents will be encouraged to support the school in:
 - reinforcing the online safety messages provided to pupils in school
 - following guidance on the appropriate use of digital and video images taken at school events and in their access to parents sections on the school's website, learning platforms and online pupil records
 - following the school's guidance on the use of their children's personal devices in the school

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)
- National Online Safety- [National Online Safety](#)
- Commonsense Media - [Commonsense Media](#)

3.7 Pupils

Pupils are responsible for using the school digital technology systems in accordance with the learner AUA and Online Safety Policy.

- They should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They should know what to do if they, or someone they know, feels vulnerable when using online technology.
- Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related in any way to their membership of the school.

3.7 Online Safety meeting group

- The Online Safety meeting is formed of a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy, including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.
- The Online Safety Group has the following members:
 - Online Safety Governor, Chair of Governors
 - Head teacher, DSL
 - Online Safety Coordinator
 - Deputy Head
 - SENDCo
 - Computing Coordinator
 - Computing TA

- Where necessary, the IT Manager will also be asked to join/ contribute to meetings.

-

Members of the group meeting will assist the OSL with:

- the production, review and monitoring of the school Online Safety Policy and relevant procedures
- the production, review and monitoring of the school's filtering policy and relevant procedures including requests for filtering changes
- mapping and reviewing the online safety curricular provision
- monitoring the school's network, internet, filtering and incident logs (where possible)
- encouraging the contribution of learners to staff awareness, emerging trends and online safety provision
- consulting stakeholders – including parents and pupils about the online safety provision

3.8 Visitors and members of the community

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. If appropriate, they will be expected to agree to the terms on acceptable use

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

- Pupils will be taught a broad range of lessons provided by: National Online Safety- [National Online Safety](#)

All schools have to teach:

- [Relationships education and health education](#) in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects, where relevant.

Across the school, the National Online Safety Platform will be used to ensure teaching is robust, up to date and appropriate for the age of the children it is targeted towards. All staff will ensure that they are using this platform to deliver focused, supportive teaching related to Online Safety and will work collaboratively with the Online Safety Coordinator to address any concerns or areas that they/ their class need support with.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school's online safety provision and should be effectively threaded through the appropriate pillars in other curriculum areas.
- Pupils should be helped to understand the need for the 'Pupil Acceptable Use Agreement' and encouraged to adopt safe and responsible use both within and outside school.
- The school curriculum is designed and written with reference to the key documents listed below, ensuring breadth and progression in the content to reflect the different and escalating risks that pupils face and covering the principles of online safety:
 - [Teaching online safety in schools \(DfE Published June 2019/updated January 2023\)](#)
 - [Education for a Connected World framework \(2020 Edition published by the UK Council for Internet Safety\)](#)
 - [Computing Curriculum \(DfE 2013\)](#)
 - National Online Safety- [National Online Safety](#)
- To ensure the quality of learning and outcomes, the online safety curriculum should be broad, up-to-date, provide opportunities for creative activities and context-relevant with agreed objectives, leading to clear and evidenced outcomes.
- Given the rapid changes in this area the school subscribes to the National Online Safety platform to ensure staff have up to date knowledge and resources to allow them to effectively teach.
- Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience. This includes:
 - how to use technology safely, responsibly, respectfully and securely
 - where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of the information.
- As part of the relationship and health education curriculum, pupils are taught about online safety and harms. This includes being taught:
 - what positive, healthy and respectful online relationships look like
 - the effects of online actions on others
 - how to recognise and display respectful behaviours on line
- Key on line safety messages should also be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would require them to access sites normally blocked by the school's filtering system. In such cases, staff can request that filters can be temporarily removed from those sites for the period of study. Any request to do so, should be auditable, with clear reasons for the need and in line with the school's procedures.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

Contribution of pupils

- The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised:
 - through mechanisms to canvass pupil feedback and opinions- questions linked to life online and online experiences within pupil voice questionnaires
 - by the appointment of Digital Leaders to work and support across the school
 - by pupil representation on the Online Safety Group- this is generally through the yearly Digital Leaders or children within other key roles
 - by pupils contributing to the writing and updating of the pupil AUA
 - pupils contributing to online safety events with the wider school community, e.g. Parent Information evenings, Online Safety newsletters and Safer Internet Day

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters, bi-termly Online Safety Newsletters or other communications home, and in information via our website, ParentMail and social media platforms. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings, where staff feel that it is necessary or there has been a concern.

The Online Safety Coordinator will lead at least one parent talk, focused on Online Safety, per year to target specific issues and share help and guidance to the wider school community.

Parents will also be given access to the National Online Safety Platform, through the school's subscription, to ensure they can access guides, training and up to date advice about a broad range of online safety related concerns.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DDSL.

Concerns or queries about this policy can be raised with any member of staff or the head teacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. This may take the form of information within the Online Safety Newsletter, specific guides or direction to training courses through the National Online Safety Platform.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DDSL and Head teacher will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will consistently monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. This will include alters linked to key phrases and language with clear linked to harmful and inappropriate material and also a termly review of the logs by the IT Manager and OSL.

More information is set out in the acceptable use agreements

8. Technology in school -

The school is responsible for ensuring that its infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The network IT manager works alongside the Online Safety Coordinator to make sure systems and procedures are robust.

a. Filtering

- The school's filtering procedures are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.
- The school uses a filtering service to manage access to content across its systems for all users. The filtering provided meets the standards defined in the [UK Safer Internet Centre Appropriate filtering](#) .
- Access to online content and services is managed for all users.
- Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content.
- There is a clear process in place to deal with requests for filtering changes
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon..
- If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site .
- Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

b. Monitoring

- The school has monitoring systems in place to protect the school, systems and users:
 - the school monitors all network use across all its devices and services
 - an appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored and the OSL, School Business Manager and IT Manager are responsible for managing the monitoring strategy and processes
 - there are effective protocols in place to report abuse/misuse and there is a clear process for prioritising response to alerts that require rapid safeguarding intervention
 - management of serious safeguarding alerts is consistent with safeguarding policy and practice
 - technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.
- The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment including:
 - physical monitoring (adult supervision in the classroom)
 - internet use is logged, regularly monitored and reviewed
 - filtering logs are regularly analysed and breaches are reported to senior leaders
 - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
 - where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

c. Technical security

- The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the School Business Manager and will be reviewed, at least annually, by the SLT
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the School Business Manager and passwords should long
- All users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.
- The master account passwords for the school systems are kept in a secure place, e.g. school safe.
- Records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user and password requirements for learners at Key Stage 2 should increase as learners progress through school.
- The school's Computing Lead will work in collaboration with the School Business Manager and IT Manager to ensure that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- Appropriate procedures, systems and security measures are in place:
 - for users to report any actual/potential technical incident or security breach
 - to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts, which might threaten the security of the school systems and data, which are regularly tested)
 - to protect the school's infrastructure and individual workstations with up-to-date endpoint (anti-virus software)
 - for the provision of temporary access of 'guests' (trainee/supply teachers and visitors) onto the school's system
 - regarding the personal use of school devices outside of school for all potential users
 - to prevent the authorised sharing of personal data unless safely encrypted or otherwise secured

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 and pupils need to be aware of the risks and legal implications associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

- The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Any images of pupils should only be taken on a school device. The personal device of staff/volunteers must not be used, except in an emergency or in compliance with exceptions within the school's "Management of Social Media Agreement" which key members of leadership staff sign and comply with.
- Staff/volunteers must be aware of those learners whose images must not be taken/published and any images of pupils should
- In accordance with guidance from the Information Commissioner's Office (ICO), parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents comment on any activities

involving other pupils in the digital/video images. This is clearly laid out in the acceptable use agreement for parents. However, there may be occasions where the school requests that parents do not take pictures or videos, but this will only be done if felt absolutely necessary and the school requests that parents are supportive and comply with such requests.

- The school withholds the right to remove children from photos before pictures are taken if the child is not allowed to have photos taken by the wish of the parent or for child protection.
- Staff and volunteers are allowed to take digital /video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of those images.
- As required by the Data Protection Act, written permission from parents will be obtained before photographs of pupils are taken for use in school or published on the school website/social media. Parents will be informed of the purposes for the use of the images, how they will be stored and for how long, in line the Data Protection and Secure Data Handling .
- Photographs published on the school website, or elsewhere, that include pupils will be carefully selected and will comply with good practice guidance on the use of such images.
- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs.
- 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupil's work can only be published with the permission of the pupil and parents.

Online publishing

- The school communicates with parents and the wider community and promotes the school through:
 - the school's website
 - social media
 - online newsletters
 - ParentMail
- The school website is managed by the IT Manager, Online Safety Lead and Computing TA
- The school ensures that the Online Safety Policy has been followed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information, thus ensuring that there is least risk to members of the school community, through such publications.

Data protection

- The school has a comprehensive 'Data Protection and Secure Data Handling Policy' written with reference to current legislation and guidance as issued by the Information Commissioner's Office, which clearly details the school's responsibilities and its staff.
- The school has appointed an appropriate Data Protection Officer who has an effective understanding of data protection law and is free from any conflict of interest.

9. Social Media

School use:

- The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:
 - ensuring that personal information is not published
 - education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
 - clear reporting guidance, including responsibilities, procedures and sanctions
 - risk assessment, including legal risk
 - guidance for learners and parents
- School staff should ensure that:
 - no reference should be made in social media to learners, parents or school staff
 - they do not engage in online discussion on personal matters relating to members of the school community
 - personal opinions should not be attributed to the school
 - security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
 - they act as positive role models in their use of social media
- When official school social media accounts are established, there should be:
 - a process for approval by senior leaders
 - clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
 - a code of behaviour for users of the accounts (acceptable use agreements)
 - systems for reporting and dealing with abuse and misuse
 - understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of social media

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

See the school's Social Networking Policy for further information

10. Reporting and Responding

- It is more than likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that the members of the school community are aware that incidents have been dealt with. Such incidents of misuse will be dealt with through the school's normal behaviour and disciplinary procedures.

- There may however be occasions when the school has to respond to reports of illegal misuse and, whilst the school will take all reasonable precautions to ensure online safety for all school users, we recognise that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.
- All staff will be made aware of the Appendices E and F: “Online Safety Incident” (Appendix E) and “Responding to Incidents of misuse” (Appendix F).
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously, dealt with effectively and that there are support strategies in place (e.g. peer support) for those reporting or affected by an online safety incident.
- The school will ensure that:
 - there are clear reporting routes which are understood and followed by all member of the school community, which are consistent with the school's safeguarding procedures (including the management of allegations) as well as the school's policies on whistleblowing and complaints
 - all members of the school community are aware of the need to report online safety issues/incidents
 - reports will be dealt with as soon as is practically possible, once they are received
 - those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as relevant
- the DSL and OSL, together with other responsible staff, will have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, (see flowchart and user actions chart in Appendix F) the incident must be escalated through the agreed school safeguarding procedures.
- Incidents should be logged using CPOMs and then will be recorded and audited through a separate Online Safety Log kept by the OSL.

11. Pupils using mobile devices in school

Pupils in years 4, 5 and 6 may bring mobile devices into school (if they walk home unaccompanied), but are not permitted to use them during:

- Lessons
- Break times/ Lunchtimes
- Clubs before or after school, or any other activities organised by the school

Pupils that bring mobile devices into school must first have a signed agreement, completed by their parents/ carers, and must comply with the school rules on mobile devices by giving them to their class teacher to be kept in a locked box for the duration of the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

12. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager or a member of SLT.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our School Behaviour Policy and Acceptable Use Agreements. 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.

11. 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, staff newsletters and staff meetings).

Annual training will be provided through the school's [National Online Safety](#) subscription. Additional training (E.g. Cyber security) will be given when advice comes from the DfE.

- All staff will receive online safety training and understand their responsibilities, as outlined in this policy.
- The OSC will receive regular updates through attendance at external training events (e.g. from the South West Grid for Learning (National Online Safety SWGfL)/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- The OSC will provide advice, guidance and training to individuals as required.
- Training to all staff will be offered as follows:
 - a planned programme of formal online safety and data protection training will be made available to all staff, which will be regularly updated and reinforced
 - the training will be an integral part of the school's annual safeguarding and data protection training for all staff

- training will include explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements/Code of Conduct
- Where staff are unsure of their responsibilities or recognise a lack of understanding and therefore a need for further training, they must raise this with their line manager..
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings and/or INSET days as required.

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 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 the risks up
- 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 and DDSs 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, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DDSs log behaviour and safeguarding issues related to online safety and feeds these back, with relevant actions and follow up policy adaptations, to the Safeguarding Committee and Online Safety Committee.

This policy will be reviewed every year by the Online Safety Coordinator/ DDSL. At every review, the policy will be shared with the Online Safety Group which includes members of the Governing Body. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy