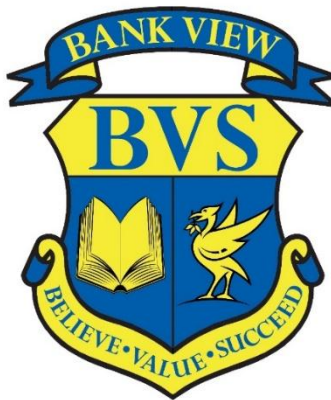


## Bank View School



## Online Safety Policy

### Document Status

<b>Review Period</b>	Annually
<b>Person Responsible for Policy</b>	ICT & Network Manager
<b>Date Reviewed and Approved by Governing Board</b>	November 2025
<b>Next Schedule Date for Review</b>	November 2026

## Policy Aims

Bank View School is committed to safeguarding children and promoting children's welfare and expects all staff, governors, volunteers and visitors to share this commitment and maintain a vigilant and safe environment. Everyone has a responsibility to act, without delay, to protect children by reporting anything that might suggest a child is being abused or neglected. It is our willingness to work safely and challenge inappropriate behaviours that underpins this commitment. The school seeks to work in partnership with families and other agencies to improve the outcomes for children who are vulnerable or in need.

This Online Safety Policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school 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).

It is essential that our children are safeguarded from potentially harmful and inappropriate online material. Our school implements a whole school approach to online safety that sets out to protect and educate both children and staff in their use of digital technologies alongside establishing mechanisms to identify, intervene in and escalate any concerns, recognising that many children and young people have unlimited and unrestricted access to the internet via mobile phone and other digital devices.

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

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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, 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 (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

## Legislation & 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 [Cyberbullying: 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.

## 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. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within our school.

## The Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Link Online Safety Governor, who will receive regular information about online safety incidents and

monitoring reports and report back to the FGB. The role of Online Safety Governor will include:

- Regular meetings with the Senior Designated Safeguarding Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Reporting to the FGB
- Receiving (at least) basic cyber-security training to enable the Governors to check that the school meets the DfE Cyber-Security Standards
- Ensure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- Ensure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children
- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with ICT staff about what needs to be done to support the school in meeting those standards, which include:
  - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
  - Reviewing filtering and monitoring provisions at least annually
  - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
  - Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

## The Principal and Senior Leaders

- The Principal 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 is held by the Senior Designated Safeguarding Lead, as defined in Keeping Children Safe in Education
- The Principal and (at least) another member of the senior leadership team 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.
- The Principal/Senior Leaders are responsible for ensuring that the Senior Designated Safeguarding Lead, ICT team and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Principal/Senior Leaders 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 Principal/Senior Leaders will receive regular monitoring reports from the Senior Designated Safeguarding Lead
- The Principal/Senior Leaders will work with the Link Governor, the Senior Designated Safeguarding Lead (SDSL) and ICT team in all aspects of filtering and monitoring.

## The Senior Designated Safeguarding Lead (SDSL)

Keeping Children Safe in Education states that:

“The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”

They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”

They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online.”

Details of the school’s Senior Designated Safeguarding Lead (SDSL) and deputies are set out in our Child Protection and Safeguarding Policies, as well as relevant job descriptions.

The SDSL will:

- Hold the lead responsibility for online safety, within their safeguarding role

- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meet regularly with the Link Online Safety Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- Attend relevant Governing Body meetings/groups
- Report regularly to Principal/Senior Leadership Team
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- Liaise with staff and ICT on matters of safety and safeguarding and welfare (including online and digital safety)
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Work with the ICT & Network Manager to make sure the appropriate systems and processes are in place
- Work with the Principal, ICT & Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Have a leading role in establishing and reviewing the school online safety policies/ documents/curriculum plans
- Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Promote an awareness of and commitment to online safety education/awareness raising across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Provide (or identify sources of) training and advice for all stakeholders
- Liaise with (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined in Keeping Children Safe in Education:
  - Content
  - Contact
  - Conduct
  - Commerce

This list is not intended to be exhaustive.

## **The ICT & Network Manager and ICT Technicians**

The ICT & Network Manager and ICT Technicians are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

The ICT team should work with the Senior Leadership Team and SDSL to:

- Procure systems
- Identify risk
- Carry out reviews
- Carry out checks

## **All Staff and Volunteers**

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood and signed the staff acceptable use agreement (AUA)
- They immediately report any suspected misuse or problem to the SDSL for investigation/action, in line with the school safeguarding procedures
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices

- In lessons where internet use is pre-planned 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

This list is not intended to be exhaustive.

## Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the pupils acceptable use agreement
- Publish information about appropriate use of social media relating to posts concerning the school
- Seeking their permissions concerning digital images, cloud services etc
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to pupils in school
- The use of their children's personal devices in the school (where this is allowed)

Parents/Carers are expected to:

- Notify a member of staff or the Principal 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/carers 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](#)

## Visitors and Members of the Community

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

Our school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

## Educating Pupils about Online Safety

Pupils are responsible for:

- Using the school's digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology
- 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 to their membership of the school.

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

All schools have to teach:

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

[Relationships and sex education and health education](#) in secondary schools

In Key Stage (KS) 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 (KS) 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.

In KS3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns.

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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

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

### **Educating Parents/Carers about Online Safety**

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers. Online safety will also be covered during parents' evenings. The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the SDSL. Concerns or queries about this policy can be raised with any member of staff or the Principal.

### **Cyber-Bullying 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school anti-bullying policy.)

### **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. Teachers will discuss cyber-bullying with their tutor groups.

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/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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 SDSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### **Examining Electronic Devices**

The Principal and any member of staff authorised to do so by the Principal can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
  - Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Principal/SLT or SDSL
  - Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
  - Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the SDSL/Principal/other member of the Senior Leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
  - Not view the image
  - Confiscate the device and report the incident to the SDSL (or equivalent) immediately, who will decide what to do next. The SDSL will make the decision in line with the DfE's latest guidance on [searching, screening and confiscation in schools - GOV.UK](#) and the UK Council for Internet Safety (UKCIS) guidance on [Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK](#)

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

- The DfE's latest guidance on [searching, screening and confiscation in schools - GOV.UK](#) UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK](#)
- Our Relationship and Behaviour policy.

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

### **Artificial intelligence (AI)**

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Bank View 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.

Bank View will treat any use of AI to bully pupils in line with our anti-bullying/relationship and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Bank View.

### **Acceptable Use of the Internet in School**

The school has defined what it regards as acceptable/unacceptable use through its acceptable use agreements. An acceptable use agreement is a document that outlines a school's expectations on the responsible use of technology by its users.

All pupils, parents/carers, 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.

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

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- Any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community users should immediately report to a nominated person - in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media.
- 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 monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

### **Pupils Using Mobile Devices**

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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.

### **Staff using work devices outside of 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 using strong passwords
- 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.

Staff members must not use the device in any way that would violate the school's terms of acceptable use policy/agreement.

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 team.

### **Reporting and Responding**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. 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 disciplinary procedures / 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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 and deputies 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.

### **Monitoring Arrangements**

The SDSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by ICT & Network Manager. At every review, the policy will be shared with the Governing Body.

## **Links with other Policies**

This Online Safety Policy is linked to our:

Child Protection Policy

Anti-Bullying Policy

Relationship and Behaviour Policy

Staff Disciplinary Policy & Procedures

Data Protection Policy

Social Media Policy