Online and E-Safety policy

Our Lady of Sion School

Approved by:	Governors	**Date:**
Last reviewed on:	October 2021	
Next review due by:	October 2022	

1. Aims

Keeping our school community safe is at the centre of everything we do.

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

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, 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 (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 scam

2. 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 – (age appropriate provision)
- 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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Sue Coldwell who is our Safeguarding Governor, working very closely with the DSL.

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 (appendix 3)
- 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 headteacher

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

3.3 The designated safeguarding lead

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

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, 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 (see appendix 5) 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 and recorded on our pastoral system, CPOMS.

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 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 weekly 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

This list is not intended to be exhaustive.

3.5 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure 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
- 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 headteacher 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 (appendices 1 and 2)
- 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

3.7 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 (appendix 3).

4. Educating pupils about online safety

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

At Our Lady of Sion School, online safety is taught and explored through:

PSHEE Curriculum (whole school)

Assembly Programme

Staying Safe area of the Learning Platform

National focus days such as Internet Safety Day

Information sent to tutors and parents around safeguarding the use of particular apps and websites popular with young people

Our areas of study are also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

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 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

In **Key Stage 3**, 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 **Key Stage 4** 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 which 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. Drawing young people's attention to the issues of "Fake News" "trolling" "cat-fishing" and addiction (amongst other concerns) is a key part of helping our students to remain safe and well – mentally and physically.

Young people spend a lot of time on social media. They are also more susceptible to peer pressure, low-self-esteem and mental ill-health. A number of studies have found associations between increased social media use and depression, anxiety, sleep problems, eating concerns, and suicide risk. Certain characteristics of social media may contribute to these negative effects.

About social media for children and teenagers

Social media platforms popular among young people
include Facebook, Twitter, WhatsApp, Instagram, Pinterest, Snapchat and TikTok.

Online multiplayer games, like World of Warcraft, League of Legends, Clash of Clans and The Sims are also important social media spaces for young people. And gaming chat sites are popular ways for young people to connect with others who share their particular gaming interests.

Using social media means **uploading and sharing content**. This includes:

- creating online profiles
- posting comments or chatting
- uploading photos and videos

- reacting to or 'liking' other people's posts
- sharing links
- tagging photos and content
- creating and sharing game modifications
- remixing or changing existing content and sharing it.

Social media: risks

Social media can also pose risks:

- being exposed to inappropriate or upsetting content, like mean, aggressive, violent or sexual comments or images
- uploading inappropriate content, like embarrassing or provocative photos or videos of themselves or others
- sharing personal information with strangers – for example, phone numbers, date of birth or location
- cyberbullying
- exposure to too much targeted advertising and marketing
- data-breaches, like having their data sold on to other organisations.

Managing social media risks for children and teenagers

Talking about social media use
Talking is the best way to protect our students from social media risks and ensure their internet safety. Talking gives us the opportunity to help young people:

- work out how they want to treat other people and be treated online – for example, you can encourage young people to make only positive comments
- understand the risks involved in using social media – for example, young people might be tagged in an embarrassing photo taken at a party
- learn how to navigate the risks – for example, if a young person posts an identifiable selfie, they can reduce risk by not including any other personal information
- learn what to do if people ask for personal details, are mean or abusive online, post embarrassing photos of someone, or share information that links back to them.

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

Online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. The School will normally block/filter access to social networking sites via the School network. Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are taught in PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The School follows general rules on the use of social media and social networking sites in School:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- They are all made fully aware of the School's code of conduct regarding the use of the intranet

- Any social media sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official School blogs created by staff or students/year groups/School clubs as part of the School curriculum will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory.
- The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately.
- Guidance for the safe the safe and professional behaviour of staff online is provided through the staff code of conduct and Safeguarding Policy

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (Staying Safe Area on FireFly).

This policy will also be made available to parents via our website.

Online safety will also be covered during parents' evenings where possible and at additional meetings for parents throughout the academic year.

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

Concerns or queries about this policy can be raised with the Headteacher and/or the Deputy Headteacher.

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 and Form 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, RSE, 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 annual safeguarding training (see section 11 for more detail).

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 DSL 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

In Our Lady of Sion School, the DSL or Deputy DSLs should make this decision as this is a decision that can only be taken after considerable thought and a full assessment of the "good reason" to do so.

If inappropriate material is found on the device, it is up to 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 (appendices 1-3). 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 monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Junior School

Pupils in the Junior School are not permitted to bring mobile devices into school. If any mobile phones are brought into school they should be handed to the office for safe keeping until the end of the school day. If a pupil is seen with a mobile phone in the Junior School, it will be confiscated and returned to the parent at the end of the school day.

Senior School

For students in Years 7 to 11, mobile phones should be switched off and kept either in school lockers or bags during the school day. Exceptions may be permitted only in exceptional circumstances if the parent/carer specifically requests it. Such requests will be handled on a case-by-case basis and should be directed to the Headteacher.

Parents/carers are requested that in cases of emergency they contact the school first so we are aware of any potential issues and may make the necessary arrangements.

Students in Years 12 & 13 may use their phone out of sight of the main population of school. They should use phones only when absolutely necessary. Staff have the right to challenge the use.

When express permission has been given by the teacher students may use their mobile phones in the classroom. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.

Mobile phones should not be used to make calls, send text messages, surf the internet, take photos or use any other application during the school day unless the class teacher has given permission. This is an important aspect of ensuring our child are safeguarded during the school day.

Using a mobile phone to bully and threaten other students is unacceptable. Cyber bullying will not be tolerated. In some cases it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given.

It is forbidden for students to "gang up" on another student and use their mobile phones to take videos and pictures to denigrate and humiliate that student and then send the pictures to other students or upload it to a website for public viewing. This also includes using mobile phones to photograph or film any student, member of staff or visitor without their consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

Students should protect their phone numbers by only giving them to close friends and keeping a note of who they have given them to. This can help protect the student's number from falling into the wrong hands and guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

Students should mark their mobile phone clearly with their names and are advised to register their details with the network provider.

To reduce the risk of theft during school hours, students who carry mobile phones are advised to keep them well concealed throughout the school day.

Mobile phones that are found in the school must be handed to the school office.

The school accepts no responsibility for replacing lost, stolen or damaged mobile phones whether in school, or while travelling to and from school.

It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones. Students must keep their password/pin confidential. Mobile phones and/or passwords should not be shared.

Mobile phones are banned from all examinations and controlled assessments. Students are expected to hand phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will be dealt with in line with exam board guidelines.

Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, 'sexting' – which is the sending of personal imagery – is also a criminal offence.

The use of mobile phones by students on School trips is at the discretion of the trip leader.

- Staff personal mobile devices must never be used to take photographs or record students either in school or off-site including in the EYFS setting.
- Staff should never use their personal mobile phone to contact students.
- School equipment must always be used for these circumstances.
- Personal mobile phones should be switched off or on silent during School hours.
- Any breach of School policy may result in disciplinary action against that member of staff.

- Mobile phone and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:
- they can make pupils and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.
- Many mobile phones are able to access 3G and 4G networks which enable pupils to bypass the school's web filtering system.
- We acknowledge that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently. We also recognise the importance of the technologies present in modern mobile phones such as internet access, cameras and MP3 playback and may wish to utilise these functions to support teaching and learning in a controlled environment. In order to safeguard our pupils throughout the school day the following acceptable use procedures are in place.
- Students in the Junior School are not permitted to bring mobile devices into school. If any mobile phones are brought into school they should be handed to the office for safe keeping until the end of the school day. Students in the Senior School are permitted to bring mobile devices into school but by doing so; they agree to abide by our acceptable use rules. **Parents are not allowed to use their mobile devices within the EYFS setting and there are notices informing visitors of this on all the entry points.**

Sharing nudes and semi-nudes: how to respond to an incident: An overview for all staff working in education settings in England

All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) or equivalent and managed in line with your setting's child protection policies.

The appropriate safeguarding lead person should be familiar with the full 2020 guidance from the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people and should not refer to this summary instead of the full guidance.

Full advice is found here:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview

What do we mean by sharing nudes and semi-nudes?

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18.

This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline.

Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately.

Your setting's child protection policy should outline codes of practice to be followed.

• Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – this is illegal. ***In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image in order to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).***

• If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.

• Do not delete the imagery or ask the young person to delete it.

• Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).

• Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.

• Do not say or do anything to blame or shame any young people involved.

• Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

Emails

The School uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Access in School to external personal email accounts may be blocked.

The School has the right to monitor emails and their contents but will only do so if there is suspicion of inappropriate use. Staff should be aware of the following when using email in School:

• Staff should only use official School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.

• Emails sent from School accounts should be professionally and carefully written. Staff are representing the School at all times and should take this into account when entering into any email communications.

• For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their line manager or a senior member of staff.

• Staff must tell their manager or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

• The forwarding of chain messages is not permitted in School.

Students should be aware of the following when using email in School, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

• All pupils are provided with a School email account and pupils may only use approved email accounts on the School system.

• Pupils should not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases will be restricted.

• Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

Policy and guidance of safe use of children's photographs and work

Photographs and pupils' work bring our School to life, showcase our students' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material. Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. (As per parental contract).

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the School will be used in public and children may not be approached or photographed while in School or doing School activities without the School's permission. The School follows general rules on the use of photographs of individual children:

- Consent from parents will cover the use of images in:
- Use in the school's promotional material such as the prospectus, the website or social media
- Press and media purposes
- Educational purposes as part of the curriculum or extra-curricular activities.
- Unpublished electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed.
- Photographs of activities, which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including in newspapers, full names will not be published alongside images of the child without the written permission from parents.
- Groups may be referred to collectively by year group or form name. Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in. Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.
- Only official school cameras may be used to take images

9. 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, as set out in appendix 3.

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 DSL or the ICT manager].

10. 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 policies on [behaviour and ICT and internet acceptable use.

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 and/or 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 and the LADO.

11. Training and Induction

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 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 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. These are logged on CPOMS and are reviewed with the Chair of Governors termly or sooner where required.

This policy will be reviewed every year by the Governors and the SLT (Headteacher with DSL advice)

At every review, the policy will be shared with the governing board. The review 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/Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- PSHEE
- RSE

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**