Newbottle and Charlton
C.E.V.A. Primary School
Every Person Matters, Every Moment Counts
'I can do all this through him that gives me strength'

Charlton
Banbury
Oxon
OX17 3DN

Telephone/Fax:
(01295) 811480

Email: bursar@newbottle.northants-ecl.gov.uk

Head Teacher:
Mr Peter Smith

Chair of Governors:
Lady Deborah Hayter

E-SAFETY POLICY

(Non-Statutory – Annual Review)

Reviewed & adopted by the Resources Committee on [Date]: *(As delegated by the FGB)*	18 March 2021
Reviewed by:	Resources Committee
Chair of Governors Signature:	
Date of next review:	March 2022

Newbottle and Charlton C.E. V.A. Primary School

Newbottle & Charlton CEVA Primary School seeks to create an environment that reflects our Christian ethos, providing safe, happy and challenging working conditions for all members of the school. This environment is exemplified by our school values and wheel with hope, dignity, wisdom and community at its hub.

Policy Statement

ICT and the internet are an integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media, including Facebook and Twitter, Instagram, snapchat
- Smart phones
- Tablets and IPads
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Video broadcasting
- Blogs and Wikis
- Email, Instant Messaging and Chat Rooms- Including Whatsapp
- Apps on various devices
- Bluetooth devices- Including voice activated smart speakers

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial.

All schools have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff continue to be protected.

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Scope of policy

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.

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or pupil use of personal devices, such as mobile phones or ipads/tablets which are brought onto school grounds. This policy is also applicable where staff or individuals have been provided with school issued devices for use off-site, such as school laptop or work mobile phone. E-safety includes use on a range of electronic devices as well as when working online.

Responsibilities

Governors

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

The governing body will co-ordinate 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 the nominated safeguarding governor: Lady Deborah Hayter.

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

Headteacher/DSL

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

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

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

- Working with other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 1) 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
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the governing body if there are any incidents (as part of the safeguarding report at every meeting).

Network Technical Staff

As the school is using an outside contractor for technical services, it is the responsibility of the school to ensure that the managed service provider carries out all of the safety measures that would be expected of the school's technical staff, including being provided with the School Online Safety Policy and Staff AUP (acceptable use policy).

The Online Safety Lead who is also the DSL and headteacher to establish and review school online safety policies and documents.

The Online Safety Lead (working with the outside contractor) for ensuring:

- that the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- that anti-virus software is installed and maintained on all school machines and portable devices.
- that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety Lead and the Designated Person for Safeguarding.
- that any problems or faults relating to filtering are reported to the technicians via an email immediately which will recorded as a incident.
- Online reports will be sent to the Online Safety Lead from the Safewatch filtering system, any incidents will be discussed with DDSL,

and a log will be created. Technical staff will be contacted if changes will be made to how all stakeholders access certain websites or apps.
- that he/she keeps up to date with online safety technical information in order to maintain the security of the school network and safeguard children and young people.
- that the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead.

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
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 1) 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

Parents and Carers

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
- Support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.
- Parents and carers can seek further guidance on keeping children safe online on the school's website safeguarding page and on the following organisations and websites:
- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

Every month guidance will be shared with parents as part of the school newsletter with current guidance and online safety top tips.

Online Safety parent/carer sessions are run regularly to raise awareness of key internet safety issues and highlight safeguarding measures in place within school.

Wherever possible, and subject to prior arrangement, the school will endeavour to provide parents/carers without internet access to research online safety materials and resources.

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.

Children and Young People

Children and young people are responsible for:

- Annually signing agreement to, and abiding by, the Acceptable Use Rules for students
- Using the internet and technologies in a safe and responsible manner within school.
- Informing staff of any inappropriate materials, cyberbullying or contact from unknown sources (age dependant)
- Actively participating in the development and annual review of the Acceptable Use Rules.
- Key Stage Two to complete the Safewatch question when they first go on to the internet.
- Understanding the importance of adopting good online safety practice when using digital technologies out of school.

Educating Pupils about Online Safety

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

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

There will be opportunities for informal discussions with students about online risks, and strategies for protecting yourself online are built into our curriculum, to ensure that our students are armed with accurate information.

Pupils with additional learning needs: The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of Online Safety awareness sessions and internet access.

Educating Parents/Carers about Online Safety

The school will raise parents' and carers' awareness of internet safety by sending out regular letters or guides and in information regularly updated on our website. This policy will also be shared with parents.

Online Safety parent/carer sessions are run regularly to raise awareness of key internet safety issues and highlight safeguarding measures in place within school.

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 any member of staff or the head teacher.

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour 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.

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.

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.

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.

Monitoring

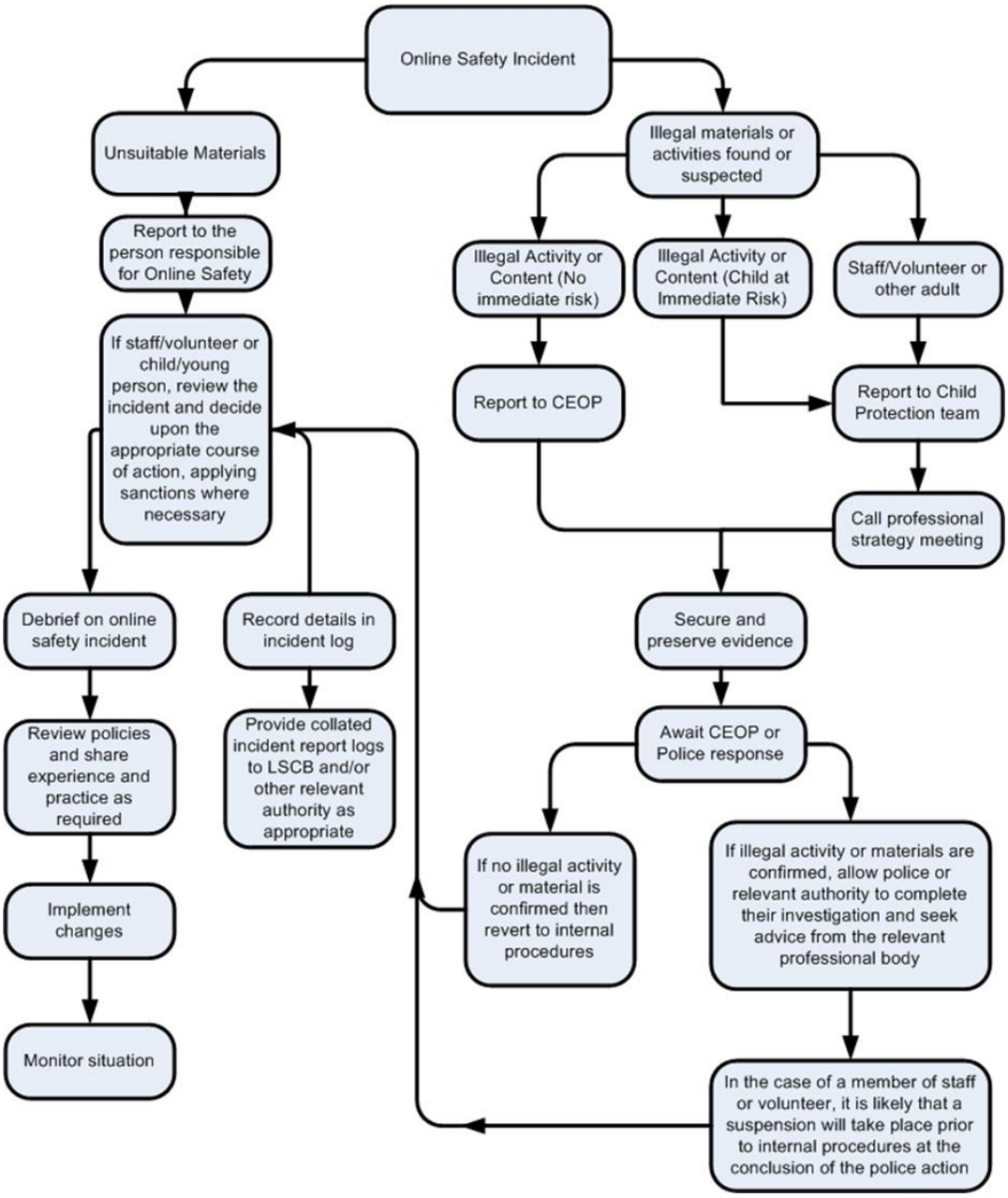
School ICT technical staff (Blue Planet) regularly monitor and record user activity, including any personal use of the school ICT system and users are made aware of this in the Acceptable Use Policy. Any websites that any stakeholders go on that are not suitable are recorded and the head teacher and is notified.

The school has installed a Watchguard Unified Threat Management Device which apart from providing enterprise level firewalling and security for the school's internet connection also provides filtering of software programs and websites.

Filtering can be both from Whitelists or Blacklists, by categories like pornography, gambling etc or by specific websites. The category database is cloud based and is continually updated giving up-to-the-minute protection. The system also logs internet activity and can produce reports and graphs based on student and teacher internet activity.

How the school will respond to issues of misuse

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Head teacher/Designated Person for Safeguarding immediately and the E-Safety Incident Flowchart followed.



In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head Teacher.

All incidents must be recorded on the Safeguarding form which will allow for monitoring, auditing and identification of specific concerns or trends.

Email Use

Staff

- The school provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and

protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

- Under no circumstances will staff members engage in any personal communications (i.e. via Hotmail or Yahoo accounts) with current or former students outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform the Head Teacher if they receive an offensive or inappropriate email via the school system.

Students

- The school provides individual email accounts for students (Yr3-6) to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information.
- Students will use their school issued email account for any school related communications, including homework or correspondence with teachers. Email content will be subject to monitoring and filtering for safeguarding purposes.
- Students will be taught from Year 2 about email safety issues, such as the risk of exposing personal information, opening attachments from unknown sources and the management of inappropriate emails. Students will also be guided in the correct tone to use in email correspondence and regularly reminded of restrictions on abusive or inappropriate content.

Both

- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the head teacher or Computing/ICT Coordinator. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head Teacher.

Managing remote access

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school network and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Only equipment with the appropriate level of security should be using for remote access (i.e. encryption on any devices where sensitive data is stored or accessed)
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.

Internet Access and Age Appropriate Filtering

Broadband Provider: BT

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored on behalf of the school by our technical support team (Blue Planet), allowing an authorised school staff member to allow or block access to site and manage user internet access.
- Age appropriate content filtering is in place across the school, ensuring that staff and pupils receive different levels of filtered internet access in line with user requirements (e.g. YouTube at staff level but blocked to students- Staff to be mindful of this when searching for websites or images on the TV screens with children).
- All users in key stage two have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering. Class log-ins are used for children in Reception and years 1 to 2.
- Any changes to filtering levels are documented by emailing the technicians and include the reason for the requested change, the date and name of staff member concerned. The email must be made with the permission from the E-safety lead or head teacher and they must be sent a copy of the email. The email will be logged with the help desk and will create an incident to action.

In addition to the above, the following safeguards are also in place

- Anti-virus and anti-spyware software is used on all network and stand-alone PCs and laptops and is updated on a regular basis.
- A unified threat management system (which includes a firewall) ensures that information about children and young people cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking.
- The report incident button is available on the SafeWatch website to allow students or staff to report online safeguarding issues.
- We have a school Wi-Fi for laptops and a guest Wi-Fi for mobile devices so that certain websites can be accessed by staff during their lunch hour in the staffroom or by governors or visitors who need the Wi-Fi for a limited amount of time. Only the Online-Safety lead and Head Teacher know the password for the school Wi-Fi to ensure that it is secure and not misused.

Staff

- Expectations for staff online conduct is addressed in the Acceptable Use Policy for School based employees.
- Staff are required to preview any websites before use, including those which are recommended to students and parents for homework support.

Use of school and personal ICT equipment

School ICT Equipment

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by Blue Planet.
- Personal or sensitive data is not stored on school devices (e.g. laptops, ipads, PC or USB Memory Sticks) unless password protected and ideally encryption software is in place. This is true also of any photographs or videos of students, such as class photos or assembly evidence.
- Time locking screensavers are in place on all devices in school to prevent unauthorised access, particularly on devices which store personal or sensitive data.
- Personal ICT equipment, such as laptops or memory sticks, must not be connected to the school network without explicit consent from the Head Teacher and a thorough virus check.

Mobile technologies including- Smart Phones

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include other cloud based services such as email and data storage including one drive from Microsoft 365.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

Student use:

- Students are not permitted to bring mobile phones/devices onto school grounds unless express permission has been granted by the Head Teacher for exceptional circumstances (e.g. independent journey to and from school)
- Where mobile phones have been allowed in the above circumstances, the device will be turned off and locked away by a responsible adult at the start of the school day and returned to the student before their homeward journey.

Staff use:

Personal mobile phones are permitted on school grounds, but should be used outside of lesson time only. It should be kept in their locker and only brought out at appropriate times not near children.

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile phones should never be used to contact children, young people or their families, nor should they be used to take videos

or photographs of students. School issued devices **only** should be used in these situations.

Laptops/ iPads/ tablets

- Staff must ensure that all sensitive school data is stored on the network (shared drive) and not solely on the laptop or device, unless the device is encrypted. In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent fine. Password protection alone is not sufficient.
- Personal use of school laptops or computing facilities, whilst on site, is left to the discretion of the Head Teacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.
- Staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

Removable Media (Memory Sticks/USB)

At times staff or visitors may require to use a memory stick to help deliver an assembly. These needed to be connected to the hall computer and regularly scan for viruses before using.

The only staff to be allowed regular use of memory sticks are the office staff and the SENCO. These will be encrypted and they are used because they often require removable media to store or access sensitive data (e.g. IEPs,) off site. Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

Photographs and Video

Digital photographs and videos are an important part of the learning experience for children and young people and, as such**,** schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and young people about the use of digital imagery within school.

- Written consent will be obtained from parents or carers before photographs or videos of young people will be taken or used within the school environment, including the school website or associated marketing material.

- Permission will be sought from any student or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Head Teacher for use of personal equipment for school related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device.
- Where photographs of students are published or displayed (e.g. on the school website) first names only will be displayed. Best practice would be to use non-identifying captions (e.g. Year 4 pupil playing football)
- Wherever possible, group shots of students will be taken, as opposed to images of individuals and images should never show young people in compromising situations or inappropriate clothing (e.g. gym kit, swimming costumes)

Video conferencing

- Permission is obtained from parents and carers prior to their child's involvement in video conferencing.
- All pupils are supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities are time logged and dated with a list of participants.

Training

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

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

The DSL and deputy 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 DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 1.

This policy will be reviewed every year by the DSL/Online Safety Lead. At every review, the policy will be shared with the Resources Committee.

Appendix 1

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**