CROWN PRIVATE SCHOOL
مدرسة كراون الخاصة

E SAFETY POLICY

'Keeping Children Safe in Education' 2020 (KCSIE)

Key Person/Dates

Designated **S**afeguarding **L**ead (**DSL**) team	Dr, Kishor Pillai – DSL Mrs. Anne Morris – Deputy DSL
Online **S**afety **C**oordinator (**OSC**)	Mr. Rajeesh/Ms Venera
Network manager / other technical support	Mr. Rajeesh/Mr Ashish
Date this policy was reviewed and by whom	August 2020 by Dr. Kishor Pillai
Date of next review and by whom	December 2020 (first initial review)

Introduction

Our pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. This presents many positive and exciting opportunities, but also challenges and risks.

The use of the latest technology is actively encouraged at Crown Private School but with this comes a responsibility to protect both pupils and the school from abuse of the system.

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2020 (KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

Objective

This policy aims to:

- Set out expectations for all CPS community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
- for the protection and benefit of the children and young people in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

Scope of the Policy

This policy applies to all members of the CPS community (including staff, proprietors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and Responsibility

Principal – Dr. Kishor Pillai

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Children's Safeguarding Partnership in Surrey guidance
- Liaise with the designated safeguarding lead and online safety coordinator on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL, Proprietors and senior management team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure the Proprietors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure all remote learning policies are kept up to date
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead – Dr. Kishor Pillai
Online Safety Coordinator – Mr. Rajeesh /Ms Venera

The DSL at CPS will take lead responsibility for Child Protection and Safeguarding (including online safety).

The Online Safety Coordinator will work alongside the DSL to ensure an effective approach within the school.

The Online Safety Coordinator and DSL will meet on a regular basis.

Key Responsibilities;

- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the School Principal, Proprietors and senior management team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Principal
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with the senior management team and the designated advisory board member for child protection to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with the Proprietors and ensure staff are aware.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children
    - it would also be advisable for all staff to be aware of onlie safety
    - cascade knowledge of risks and opportunities throughout the organisation.
    - Keep all remote learning policies up to date.

Top Management

Key responsibilities:

- Approve this policy and strategy and subsequently review its effectiveness.
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for child protection and safeguarding (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at senior management meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DSL and Principal to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated in line with advice from the Children's Safeguarding Partnership in Surrey. Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.
- Ensure appropriate filters and appropriate monitoring systems are in place.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.
- Consider a whole school approach to online safety with a clear policy on the use of mobile technology.

All Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Coordinator (OSC) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for Senior management team and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff code of conduct
- Notify the DSL/OSC if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads,

and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL/OSC what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, including the remote learning responsible user agreement for pupils, remind them about it and enforce school sanctions
- Notify the DSL/OSC of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors and other communal areas outside the classroom – let the DSL/OSC know
- Receive regular updates from the DSL/OSC and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Follow the remote learning policy and teacher protocols during any part or full school closure

PSHE Coordinator – Ms Venera

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ Relationships Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and Relationships Education.

ICT Department (Computing Curriculum Lead)

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements, including remote learning agreements.

IT Department (Network and Facilities) – Mr Rajeesh and Mr Ashish

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety coordinator to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior management team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safeguarding lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy, including the remote learning responsible use policy for pupils and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials

- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies (including remote learning policies) cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/Carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP), Including remote learning policies and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Proprietors, contractors, pupils or other parents/carers.

Parent Council – Ms Hanifa

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Proprietors, contractors, pupils or other parents/carers.

Academic/Education and Curriculum – Team Leaders

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Moral Education
- ICT

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should

encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Crown Private School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to focus on the key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

We follow the 'Education for a Connected World' framework which helps to equip children and young people for digital life. The 8 themes are also integrated into our termly assembly plans.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety coordinator / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

The school's procedures for dealing with online-safety are mostly detailed in the following policies (primarily in the first key document):

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)

Crown Private School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Principal, unless the concern is about the Principal in which case the complaint is referred to the Proprietor and the Local Authority

We will inform parents/carers of online-safety incidents involving their children, where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

System Security

Monitoring

The school reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate disciplinary action will be taken.

Property

Pupils and staff should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to a member of office staff.

Viruses

Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

System Security

- All computers and laptops are password protected. Passwords are changed on a regular basis.
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.
- Do not make deliberate attempts to disrupt or damage the school network, any device attached to it or any data stored on it or transmitted across.
- Do not alter school hardware in any way.
- Do not knowingly misuse headphones or any external devices e.g. printers, mouses.
- Do not eat or drink while using the computer.
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data.

Leaving workstations

If a person leaves their workstation for any period of time they should log out of their workstation.

INTERNET

The School recognises the benefits to using the Internet in an educational environment. The Internet facility is provided for school related activities only. The school monitors the use of the Internet.

The school internet system has a filtering and monitoring system run by ISP, Etisalat which by default and govern by UAE Law monitors and filters all website access against preset policies. Any inappropriate material, whether it be sexual, violent, extremist or illegal in nature will be blocked and the System Administrator alerted, who will in turn alert the school Designated Safeguarding Lead/ Online Safety Coordinator, as to the inappropriate material being accessed.

Viewing, retrieving or downloading of any material that the school considers inappropriate will result in appropriate disciplinary action. The school also applies LAN and Internet firewall and anti-virus app for more security

Good practice guide for staff, pupils and parents

Staff Personal Safety

It is vitally important that staff are careful about content that they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages.

Staff need to ensure that films or other material shown to children are age-appropriate.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher.

Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school branding (uniform).
- Staff must not form online friendships with pupils and parents.
- Staff must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Staff will be required to attend an annual internet safety course and ensure that they pass this information on to the children in their care.
- Staff should use their school email account for all school-related communications.
- Staff to be aware of the various members of staff responsible for Safeguarding issues – Dr. Kishor Pillai (Designated Safeguarding Lead), Ms Anne Morris (Deputy Designated Safeguarding Lead), and Mr Rajeesh (Online Safety Coordinator).
- Staff members should refer to the Staff Code of Conduct for more detailed information.

Pupil Personal safety

The school will organise internet safety lessons on a termly basis with one from an external presenter.

- Pupils must not play with or remove any cables etc that are attached to a school computer.
- Pupils will be taught how to stay safe when working online at school and at home.
- Pupils must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.

- Pupils must not post anything on any online site that can be constructed to have an adverse impact on the school's reputation.
- Pupils must not post photos of video related to the school on any internet sites including pupils, staff, parents or the school branding (uniform).
- Pupils should never reveal their full name, any address or contact details, any school or network user ID or password online, even if communicating with known acquaintances.
- Pupils should be aware that the potential exists for predators to remain entirely anonymous and easily pose as someone else.
- Pupils should employ a healthy mistrust of anyone that they "meet" online unless their identity can be verified.
- The use of chat rooms and social networking sites are not permitted in school.
- Do not arrange to meet anyone you have met on the internet - people are not always who they say they are.

Parents

- Parents will be invited to an annual e-safety evening run by an external presenter which will consist of advice and useful tips to help support them in ensuring their child's computer and internet safety at home.
- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

Inappropriate Behaviour

Bullying of another person will be treated with the highest severity.

Online, Cyber Bullying

- Lessons concerning cyber bullying to be carried out termly through the computing and PSHE curriculum.
- By cyber bullying, the School is referring to: bullying by email, messages, images, calls or other electronic communication.
- Use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites (including social networking sites).
- Hijacking or hacking email accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms or on instant messaging services.
- The use of Social Media for the use of bullying, grooming, abuse and radicalisation.

Pupils should be aware that cyber bullying is generally criminal in character and that English law does apply. The School will endeavour to resolve all matters using the School's Behaviour Policy without Police involvement but parents of victims do have the right to seek Police intervention. This will be closely linked to the School's Anti-Bullying Policy and CPS's Child Protection and Safeguarding Policy which can be read separately or in conjunction with this policy.

Email

Personal use

Email is provided for school related purposes only. The school monitors the use of email and disciplinary action may be taken if inappropriate uses of personal emails are discovered.

Status

Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. Pupils and staff should not include anything in an email that is not appropriate to be published generally. Any email message which is abusive, discriminatory on grounds of sex, race, disability, sexual orientation or religious belief, or defamatory is not permitted.

Humour

Trivial messages and jokes should not be sent or forwarded using the school email system. Not only could these cause distress to recipients but could also cause a degradation and/or damage to the School's network.

Privacy

All files and emails on the system are property of the School. As such, system administrators and staff have the right to access them if required.

Secure Documents

All emails of a sensitive or secure nature should be sent using the 'Egress' email system. Staff can find out about this by talking to a member of the office staff, the Principal or the Online Safety Coordinator, Mr. Rajeessh

Plagiarism and Copyright

Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the internet or anywhere else.

You should respect copyright. Breaking copyright laws occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner. This includes the copying of music files and CDs.

The School purchases appropriate licences where required.

Photography - Digital Images and Video

The word photography is used in this policy to include traditional photographs and digital images of any kind, still or moving.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Photography and video are familiar features of life, playing a significant role in commerce, entertainment and communication; it is commonplace in our homes and it is an important element of school life.

At CPS we feel it is vital that achievements are recognised and that pupils feel valued, proud and happy. Photography is a useful tool within school and it is employed routinely in many ways, for example; record keeping, displays, special events, teachers' lessons and the children's own work.

On occasions photos are also used for the Press, school website and other promotional purposes.

Children will only be named in photographs that are displayed within the school. We will not provide children's full names for any other purpose unless special parental consent has been received.

We are, however, sensitive to the wishes and rights of parents who may not wish their children to be photographed and who may have concerns about the use of such images.

Taking Photographs and Video

All parents are asked to give consent for photography of their child by completing a permission slip that is held on file. A register is kept of children who must not be included in press, website or any other photographic image, still or moving.

All reasonable measures will be taken to ensure that no child on the register is photographed or videoed by a visitor to school or while on an educational visit outside school. The exception to this may be photographs taken by parents at events such as concerts and church services.

From time to time we invite the Press into school to share special events and achievements within the local community. We will allow local newspapers to take photographs of children, when appropriate, provided that parental consent has been given.

Some newspapers insist that children's names must be published with their photographs. If not, they may decline to cover school events. Therefore we will normally give the children's full names (but not addresses) to newspapers only if requested by them. That is why it is important for you to tell us whether you have any objections.

Images taken by school staff

Only the school's cameras or video equipment are to be used by staff when taking photographs. All equipment must be handed in at the end of the day to the Principal's office where it is locked away until the following day.

The printing of images is always carried out on the school premises. All photographic images held on cameras will be deleted at the end of each week.

All images taken must be deemed suitable without putting the child in any compromising positions that could cause embarrassment or distress.

Under no circumstances will a camera be allowed into the bathroom areas unless a member of the Senior Management team is present. For example, if staff in the Early Years would like photos of the children washing their hands for hygiene posters a member of the Senior Management team must be present.

Photographs taken as records of events or for educational purposes may be displayed around the school. They are then archived or shredded after use.

Photographs used for evidence in the Early Years Learning Journeys will be handed to the parent at the end of the Reception year.

Photographs are not exchanged with anyone outside school, or removed for private use by any employee or volunteer.

Images taken by adults other than school staff

When a commercial photographer/filmmaker (contractor) is used we will;

- Provide a clear brief
- Issue Identification
- Inform parents and children
- Obtain consent
- Not allow unsupervised access to children

Images taken by children

The school encourages children to take photographs on school trips or on residential visits using a disposable camera as a way of recording events.

There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed. This is seen as part of the school's code of behaviour.

Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other breach of school discipline.

Under no circumstances will pupils be allowed to bring to school or take on trips any electronic devices such as tablets, smartphones, smartwatches, laptop or other computer devices which have the capability to film videos or internet access.

Should the school learn about any inappropriateness of image use involving our pupils or staff, we will immediately act and report it as we would for any other child protection issue.

Social Media

Westward School works on the principle that if we don't manage our social media reputation then someone else will.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Staff, pupils' and parents' social media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school.

Pupils and parents are not allowed* to be 'friends' with or make a friend request** to any staff, volunteers and contractors or otherwise communicate via social media.

Pupils and parents are discouraged from 'following' staff, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Principal (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

Use of mobile phones

The following rules apply for the use of personal mobile phones;

Pupils

- Pupils are not permitted to bring mobile phones, smartwatches or personally owned devices into school.
- Pupils in Year 6 who have been given permission by the Principal to walk to and from school must sign in their mobile phones at the school office when they arrive in the morning for safe-keeping in a locked location during school hours.
- Pupils must sign out their mobile at the end of the day just before leaving the school premises.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with school policy.

Staff

- The school accepts that employees will bring their mobile phones to work.
- Mobile phones and personally owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- Employees are not permitted to make/receive calls/texts during lessons or formal school time or use recording equipment on their mobile phones or personal devices to take photographs/videos of children.
- Staff use of mobile phones during the school day will normally be limited to the morning/lunch break and after school.
- Mobile phones should be switched off (or silent) and left in a safe place during lesson times. Staff should use phones in designated areas. The designated area is the Staff Room. If a private call needs to be made then a request for a room can be made to the Principal.
- Mobile phones are not permitted in areas where children are present.
- In the event that an employee has a particular reason for a specified period of time, they may request via the Principal that they leave their phone on during working hours.
- If a staff member breaches the school policy then disciplinary action may be taken as appropriate.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Mobile phones should not be used in a space where children are present unless the School phone is being used for a medical reason,

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow students / pupils to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the students / pupils. The table has been left blank for school to choose its own responses.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x			x				X
Use of mobile phones in lessons			x					x
Use of mobile phones in social time	x x							x
Taking photos on mobile phones / cameras			x	x	x			x
Use of other mobile devices eg tablets.	x					x x		
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails			x					x x
Use of messaging apps			X					x
Use of social media			x					x
Use of blogs			XX X				XXX	

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report to the 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.**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses will be provided with individual school email addresses for educational use.*

- *Pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by Senior Staff and e-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school

or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

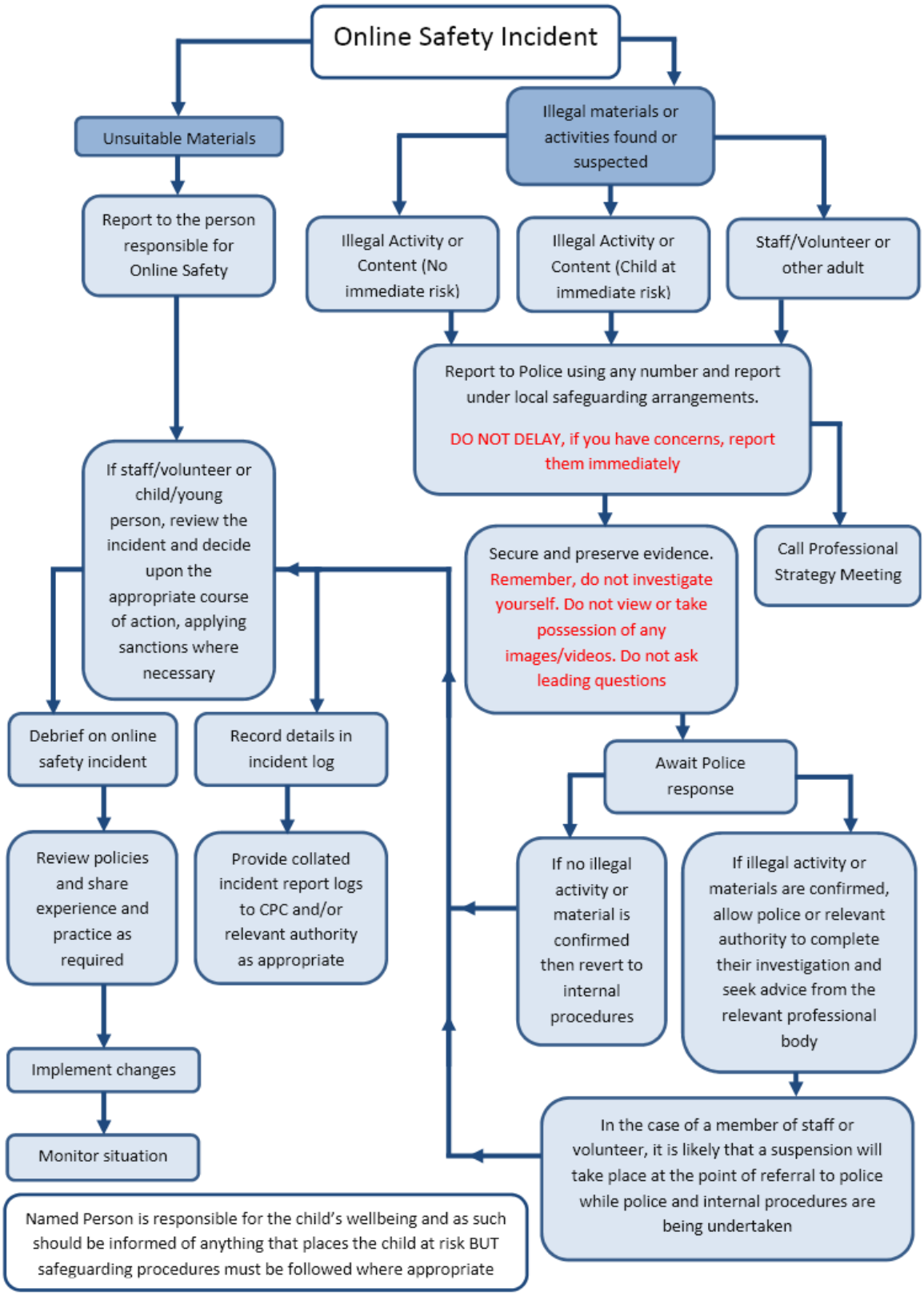
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				x	
On-line gaming (non educational)				x	
On-line gambling				x	
On-line shopping / commerce		x			
File sharing		x			
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting eg Youtube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when

infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which is potentially obscene
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions

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

Students / Pupils **Actions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons						x			
Unauthorised use of mobile phone / digital camera / other mobile device						X			
Unauthorised use of social media / messaging apps / personal email						X			
Unauthorised downloading or uploading of files							x		
Allowing others to access school network by sharing username and passwords	X								
Attempting to access or accessing the school network, using another student's / pupil's account			X			x	x	X	
Attempting to access or accessing the school network, using the account of a member of staff			X			x	x		x
Corrupting or destroying the data of other users			x			x	x		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			x	x		X
Continued infringements of the above, following previous warnings or sanctions			x	x		x	x		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			x	x		x
Using proxy sites or other means to subvert the school's 's filtering system			x			x	x		X
Accidentally accessing offensive or pornographic material and failing to report the incident			X			x	x	x	
Deliberately accessing or trying to access offensive or pornographic material			x			x	x		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x			x	x		x

Staff **Actions**

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			x	x
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		x						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X						
Careless use of personal data eg holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security rules			x			X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x			x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x				x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x				x		
Actions which could compromise the staff member's professional standing		x	x					x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x			x		
Using proxy sites or other means to subvert the school's 's filtering system		x				x		
Accidentally accessing offensive or pornographic material and failing to report the incident		x				x		
Deliberately accessing or trying to access offensive or pornographic material in school or using school hardware		x	x				x	x
Breaching copyright or licensing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x	x					x