LBBD Schools

Online Safety

Policy Template

November 2021

This Online Safety Policy, based on documents by SWGfL and LGfL, can be used by schools as a template to write their own policy.

Barking and Dagenham School Improvement Partnership (BDSIP) for London Borough of Barking and Dagenham (LBBD)

Based on documents from:
South West Grid for Learning (SWGfL)
London Grid for Learning (LGfL)

Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. It is designed to sit alongside your school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Online Safety Policy Review

The school's Online Safety Policy will operate in conjunction with other policies including Safeguarding, Behaviour, Bullying, Computing, RSHE (Relationships Education, Relationships and Sex Education and Health Education) and PSHE (Personal, social, health and economic) curriculum, Data Protection, Information Security and any Home-School Agreements.

Policy review date:	
Policy reviewed by:	
Policy approved by Governors on:	
Next policy review date (at least annually):	

Key People

Designated safeguarding lead (DSL) / team:	
Online safety lead (if different):	
Online safety / safeguarding link governor:	
RSHE / PSHE lead(s):	
Computing subject lead:	
Network manager / technical support:	
Data protection officer:	

Contents

Overview

Online safety is an integral part of safeguarding and requires a whole-school approach. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

'Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.' (Keeping Children Safe in Education (KCSIE) 2021, para 125)

Purpose of the Policy

Schools must have an online safety policy covering the safe use of internet and electronic communications technologies such as mobile phones and internet connected devices. The policy will highlight the need to educate children, young people and their families about both the benefits and risks of using technologies both in and away from the school context. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. There are additional duties under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. Revised "Keeping Children Safe in Education" guidance obliges schools and colleges in England to 'ensure appropriate filters and appropriate monitoring systems are in place.'

The school's Online Safety Policy will operate in conjunction with other policies including Safeguarding, Behaviour, Bullying, Computing, RSHE and PSHE curriculum, Data Protection, Information Security and any Home-School Agreements.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carer, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be available via the school office / network / website
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for networks activity
- Surveys / questionnaires of pupils, parents / carers and staff

Note regarding policy template:

E **It is suggested that statements with the 'E' bullet should be an essential part of the school online safety policy. There may need to be some editing to suit local requirements.**

- Round bullet points indicate optional items, which may require editing to suit local requirements.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school (in some cases the roles described may be combined).

Headteacher

E To foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding

E To take overall responsibility for the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead

E To take overall responsibility for data management and information security ensuring the school follows best practice in information handling

E To ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, and protected email systems

E To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

E To understand and make all staff aware of procedures to be followed in the event of a serious online safety incident

E To ensure the school website meets statutory requirements

- To ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised
- To receive regular monitoring reports from the Online Safety Lead
- To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)

- To ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

Designated Safeguarding Lead

E Take lead responsibility for online safety:

- 'The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety)….Whilst the activities of the designated safeguarding lead can be delegated to appropriately trained deputies, the ultimate lead responsibility… remains with the designated safeguarding lead. This responsibility should not be delegated.' (KCSIE 2021, paras 89 & 91)

Some schools may choose to combine the roles of Designated Safeguarding Lead and Online Safety Lead.

E Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online bullying
- *NB it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.*

E Facilitate training and advice for all staff on Keeping Children Safe in Education (2021), including Annex D (online safety)

E To 'liaise with staff (especially pastoral support staff, school nurses, IT technicians and SENCOs…) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.' (KCSIE 2021, page 144)

- Oversee and discuss 'appropriate filtering and monitoring' on school systems with technical teams, governors and all staff. Whilst the technical team will do the technical work, DSL should be involved in key decisions to ensure the children are kept safe but 'be careful that over-blocking does not lead to unreasonable restrictions…' (KCSIE 2021, para 122)
- Work with the headteacher and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Where the online safety lead is not the named or deputy designated safeguarding lead (DSL), ensure there is regular review and open communication between these roles and that the DSL's overarching responsibility for online safety is not compromised
- If the school is engaging online tutors, ensure they have signed the relevant AUP

Online Safety Lead

It is strongly recommended that each school should have a named member of staff with a day to day responsibility for online safety; some schools may choose to combine this with the Designated Safeguarding Lead role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of new technologies, rather than a technical member of staff – but this will be the choice of the school.

E To ensure 'an effective whole school and college approach to online safety (that) empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.' (KCSIE 2021, para 123)

- **E** To take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- **E** To have a leading role in establishing and reviewing the school online safety policies / documents
- **E** To promote an awareness and commitment to online safety throughout the school community including hard-to-reach parents
- **E** To ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life
- **E** To ensure that 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 other safeguarding incidents
- **E** To ensure the log of incidents informs future online safety developments
- **E** To stay up to date in online safety issues and legislation
- **E** To facilitate training and advice for all staff, either as part of or in addition to safeguarding training
- To communicate regularly with SLT and the designated online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
- To ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation / quarantine / lockdown (e.g. an online 'worry box' form; Tootoot or other reporting platforms)
- To promote an awareness and commitment to online safety throughout the school community, with a strong emphasis on parents and carers

Governors / Online Safety Governor

- **E** To ensure that the school has in place policies and practices to keep the children and staff safe online
- **E** To approve the Online Safety Policy and review the effectiveness of the policy
- **E** To ensure all staff undergo safeguarding and child protection training (including online safety)
- To support the school in encouraging parents and the wider community to become engaged in online safety activities
- To ask how the school has reviewed protections for pupils in the home and remote-learning procedures, rules and safeguards
- The role of the Online Safety Governor may include:
    - regular strategic reviews with the Online Safety Lead / DSL
    - attendance at the Online Safety group meetings
    - regular monitoring of online safety incident logs
    - regular monitoring of filtering / change control logs
    - reporting to relevant Governor meetings

The Governor role may be combined with that of the Child Protection / Safeguarding Governor)

All Staff (including Teaching and Support Staff)

- **E** To ensure they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices (including safeguarding provisions for home learning and remote teaching) and have read relevant sections of KCSIE 2021
- **E** To understand that online safety is a core part of safeguarding; as such it is everyone's responsibility
- **E** To read, understand, sign and adhere to the school Online Safety Policy and staff Acceptable Use Agreement, in conjunction with the school's main safeguarding policy
- **E** To record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures

- **E** To ensure that any digital communications with pupils / parents / carers should be on a professional level and only through school-based systems, e.g. not on personal email, mobile phones etc.
- **E** To embed online safety in all aspects of school life, both across the curriculum and outside the classroom
- **E** Curriculum subject leaders to identify opportunities to thread online safety through their curriculum subject and work with class teachers to implement
- To ensure that pupils understand and follow the Online Safety Policy and Pupil Acceptable Use Agreement
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular, extended school activities and home learning where relevant)
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- To ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To prepare and check online source and resources before using within the classroom
- To monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- To model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and on social media; in all aspects upholding the reputation of the school and the profession
- To be aware of security best-practice, including password 'hygiene' and phishing strategies

RSHE / PSHE Subject Leader(s)

- **E** Embed consent, mental wellbeing, healthy relationships and staying safe online into the RSHE / PSHE curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.
- Work closely with DSL and online safety lead to ensure a shared understanding of the issues, approaches and messages for RSHE / PSHE
- Work closely with the computing lead to avoid overlap and ensure a complementary whole-school approach to online safety

Computing Subject Leader

- **E** To oversee the delivery of the online safety element of the Computing curriculum, ensuring progression in the content to reflect the different and escalating risks that pupils face
- Work closely with DSL and online safety lead to ensure a shared understanding of the issues, approaches and messages for the computing curriculum
- Work closely with the RSHE / PSHE lead(s) to avoid overlap and ensure a complementary whole-school approach to online safety
- 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

Network Manager / Technical staff / Computing Subject Leader

If the school has an IT managed service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out the online safety measures that would otherwise be the responsibility of the school technical staff. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.

- **E** To 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
- **E** To report any online safety related issues that come to their attention in line with school policy
- **E** To work closely with the DSL / online safety lead / data protection officer to ensure that school systems and networks reflect school policy, ensuring they understand the consequences of existing services and of any changes to these systems
- To support the HT and DSL team as they review protections of pupils in the home and remote-learning procedures, rules and safeguards
- To support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and SLT
- To ensure the school's policy on web filtering is applied and updated on a regular basis
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To keep up to date with the school's online safety and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- To regularly monitor the use of school technology, online platforms and social media presence *(move this requirement to different role if appropriate)* and that any misuse / attempted misuse is reported in line with school policy
- To ensure that monitoring software / systems are implemented and updated as agreed in school policies
- To maintain up to date documentation of the school's online security and technical procedures
- To work with the headteacher to ensure the school website meets statutory DfE requirements *(move this requirement to different role if appropriate)*

Data Protection Officer

Further information regarding the Data Protection Officer (DPO) and General Data Protection Regulation (GDPR) should be found in the Data Protection / GDPR policy.

- **E** To oversee the data protection strategy in school, and ensure compliance with GDPR legislation
- **E** To ensure best practice in information management, i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- **E** To ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- To be aware of references to the relationship between data protection and safeguarding in key DfE documents; Keeping Children Safe in Education (2021) and Data protection: a toolkit for schools (August 2018)

Pupils

- **E** To read, understand, sign and adhere to the Pupil Acceptable Use Agreement annually
- **E** To understand the importance of reporting abuse, misuse or access to inappropriate materials, and how to do so, including any concerns about a member of school staff, supply teacher or online tutor
- **E** To know what action to take if they or someone they know feels worried or vulnerable when using online technology at school, at home or anywhere else
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, including on social media
- To treat home learning during any isolation / quarantine or closure in the same way as regular learning in school, and behave as if a teacher or parent were watching the screen

- Avoid any private communication or use of personal logins / systems to communicate with or arrange meetings with school staff or tutors
- To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To know, understand and adhere to the school policy on the use of mobile devices and digital cameras, including the taking / use of images and online bullying
- To 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

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through, e.g. parents' evenings, newsletters, website, workshops.

- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement, including the use of photographs and video images and pupils' use of the internet
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children and encourage their children to follow it
- To consult with the school if they have any concerns about their children's use of technology
- To model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media
- Encourage children to engage fully in home-learning during any period of isolation / quarantine or closure and flag any concerns

Volunteers, Contractors (including Tutors) and Community Users

- To read, understand, sign and adhere to an acceptable use policy
- To support the school in promoting online safety
- To maintain an awareness of current online safety issues and guidance
- To model safe, responsible and positive behaviours in their own use of technology
- To report any concerns to the DSL / online safety lead

Education and Training

Pupils

"Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety… Schools should consider all this as part of providing a broad and balanced curriculum." Keeping Children Safe in Education, paras 119 & 120; DfE 2021

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety message across the curriculum. The following subjects have the clearest online safety links:

- Relationships Education (Primary), Relationships and Sex Education (Secondary) and Health Education (all); also known as RSHE

- Computing
- Citizenship

In planning their online safety curriculum, schools are also advised to refer to:

- DfE Teaching Online Safety in Schools guidance (2019)
- Education for a Connected World framework (UK Council for Internet Safety, 2020)

Additional links, Keeping Children Safe in Education para 121.

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

E A planned online safety curriculum should be provided as part of RSHE / PSHE / Computing / other lessons and should be regularly revisited

E Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

E Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information (critical thinking, 'fake news')

E Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

E Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making (NB additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet)

E Pupils should be helped to understand the need for the pupil Acceptable Use Agreement, sign and follow the guidance outlined in the agreement

E Pupils should be taught and encouraged to adopt safe and responsible use of technology both within and outside school, including appropriate online behaviour and keeping personal information private

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices, e.g. use of passwords, logging-off, use of content, research skills, copyright
- Whenever overseeing the use of technology in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and age appropriateness of websites.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- (Secondary) From time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request the filter lists be adjusted for the period of study. Any request to do so should be auditable, with clear reasons for the need

Staff and Governors

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Governors are invited to online safety training events.

Training will be offered as follows:

E A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced

- **E** All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements
- An audit of the online safety training needs of all staff will be carried out regularly
- The Online Safety Lead will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy will be presented to and discussed by staff in staff meetings
- The Online Safety Lead will provide advice / guidance / training to individuals as required

Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Displays in school / at parents' evenings
- Parent / carer online safety workshop
- Curriculum activities
- High profile events and campaigns such as Safer Internet Day
- Reference to the relevant websites / publications for further support

Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experiences. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise / good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Technical Management

Infrastructure, Equipment, Security and Filtering

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy / acceptable use agreements. The school should also check their Local Authority / MAT / other relevant body policies on these technical issues.

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible, and that the policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their online safety responsibilities.

- There will be regular reviews and audits of the safety and security of the school technical systems
- The school network has user-defined policies ensuring secure documents are only accessible by specific users
- The school has educational, filtered, secure broadband connectivity
- Internet access is filtered for all users to keep users safe, including from terrorist and extremist material. Illegal content is filtered by the broadband provider, and only nominated staff are able to make a change to the filtering system
- The school will ensure, to the best of their ability, that the filtering system prevents pupils using websites designed to bypass the filtering
- The school has a secure wireless network to ensure access is restricted to school devices
- If staff or pupils come across unsuitable on-line materials, the site is reported to the appropriate person(s) in line with school policy
- The school checks their virus protection is updating regularly and informs their IT Support Service provider of any issues
- Staff and pupils have access to the school network via a login suitable to their 'role'. Staff do not share their login details. *(From Year 1 pupils should have individual logins, though the passwords may not be complex at KS1)*
- Staff access to the management information system is controlled through a separate password for data security purposes. Staff only have access to the modules they require for their role, and passwords are not shared
- The school checks that their data is backed up, and that data can be retrieved
- The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Guest accounts are only used for a short period of time by temporary staff
- Guest access to wifi is only accessible with a guest password which is changed regularly
- The school requires all users to log off when they have finished working, and to log off (or lock if not a shared computer) when leaving the computer unattended
- The school ensures that all pupil level or personal data sent over the internet is encrypted or sent using an approved system, for example DfE S2S, encrypted / secure email
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
- Pupils use a child-friendly internet search engine

Password Policy

- The school makes it clear that staff and pupils must always keep their passwords private and not share them with others
- If a password is compromised the school should be notified immediately
- Staff are required to use strong passwords for network / email / MIS
- Staff are required to change their email / MIS passwords at least twice a year

Mobile Technology (including BYOD)

If schools implement a 'bring your own device' (BYOD) policy, then this section will need to be re-written accordingly. A more detailed policy template is available from SWGfL.

- **E** Personal devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school
- **E** Staff should not use their personal device when contacting pupils or parents; there should be access to a school phone
- The school strongly advises that pupils' mobile phones should not be brought into school
- Staff who work directly with pupils should leave their mobile phones on silent and not use them in the presence of pupils
- The recording, taking and sharing of images, video and audio on any personal device is to be avoided, except where it has been explicitly agreed otherwise by the headteacher
- The school reserves the right to search the content of any mobile or handheld device on school premises where there is a reasonable suspicion that it may contain undesirable material
- Personal devices will not be used during lessons unless as part of an approved and directed curriculum-based activity

Data Protection

Further information should be available in the school Data Protection / GDPR policy.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school must ensure that:

- **E** It has a Data Protection Policy
- **E** It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records
- **E** It has paid the appropriate fee to the Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO)
- **E** It has appointed a Data Protection Officer who has a high level of understanding of data protection law and is free from any conflict of interest
- **E** It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- **E** The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- **E** It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it longer than necessary for the purposes it was collected for
- **E** Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay
- **E** The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- **E** Where special category data is processed, a lawful basis and a separate condition for processing have been identified
- **E** Data Protection Impact Assessments are carried out where necessary; for example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- **E** It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties, e.g. cloud service providers
- **E** Procedures must be in place to deal with the individual rights of the data subject, i.e. Subject access Requests to see all or part of their personal data held by the data controller

- There are clear and understood data retention policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible
- Consideration has been given to the protection of personal data when accessed using any remote access solutions
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Where personal data is stored or transferred on mobile of other devices (including USBs) these must be encrypted and password protected
- Will not transfer any school data to personal devices except as in line with school policy
- Access personal data sources and records only on secure password protected computers and other devise, ensuring that they are properly 'logged off' at the end of any session

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted, and password protected.
- The device must be encrypted, and password protected.
- The device must be protected by up-to-date virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press

- **E** Digital media should be used in accordance with the home school agreement
- The digital media release form should be reviewed annually
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website will be selected carefully and will comply with good practice guidance on the use of such images
- Pupil's work can only be published with the permission of the pupil and parents or carers

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Schools need to consider the benefit of using these technologies for education whilst reducing their risks (see **appendix 1**).

- **E** The school email service may be regarded as safe and secure and is monitored. Staff and pupils should only use the school email service to communicate with others when in school, or on school systems
- **E** Any digital communication between staff and pupils or parents / carers must be professional in tone and content, and must only take place on school approved systems. Personal email addresses or social media must not be used for these communications
- **E** Users must immediately tell an appropriate member of staff if they receive any communication which is offensive, discriminatory, threatening or bullying in nature, and should not respond to any such communication
- **E** Staff or pupil personal contact information should not be published. The contact details given online should be the school office
- Pupils should be taught about online safety issues such as the risks attached to the sharing or 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
- Pupils need to be educated in how to deal with incoming email and associated attachments
- The school should consider how e-mail from pupils to external bodies is presented and controlled
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use

Social Media – Staff (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 material online. Expectations for teachers' professional conduct are set out in Teachers Standards 2012. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in

place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools 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.

A more detailed Social Media Policy Template is available for SWGfL.

E The school has clear reporting guidance, including responsibilities, procedures and sanctions

E The school ensures that personal information is not published

E All school staff sign the Acceptable Use Agreement indicating they understand and will follow the guidance contained

- A social media risk assessment has been carried out
- School staff ensure they make no reference in social media to pupils, parents / carers or school staff
- School staff should not engage in online discussion on personal matters relating to members of the school community
- School staff should ensure that personal opinions are not attributed to the school or local authority
- School staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

When official school social media accounts are established there should be:

- A process for approval be senior leaders
- Clear processes for the administration and monitoring of these accounts
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse

Personal use:

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

Monitoring of public social media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school
- The school effectively respond to social media comments made by others according to a defined policy or process

Social Media – Pupils

- **E** The school will control access to social networking sites, and where relevant educate pupils in their safe use
- **E** Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils
- Pupils will be advised to use nicknames and avatars when using social networking sites

Incident Management

Responding to 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 / RSHE and Citizenship). General concerns must be handled in the same way as other safeguarding concerns.

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy

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. 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 **appendix 2** for Dealing with Unsuitable / Inappropriate Activities, including school actions and sanctions pro formas, and **appendix 3** for Sharing nudes and semi-nudes advice*

Some internet activity, e.g. accessing child abuse images or distributing racist materials is illegal and would obviously be banned from school. Other activities e.g. cyberbullying 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.

The usage restrictions form (**appendix 2.1**) allows schools to document whether activities are acceptable or not. If using the form, the school should agree its own responses and complete / modify the pro forma as appropriate. The form could be duplicated to define the usage for staff and pupils.

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; actions and sanctions forms (**appendix 2.2 and 2.3**) can be completed by the school once the responses have been agreed.

E If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the incident will be reported to the appropriate bodies immediately (see right hand side of **flowchart** below)

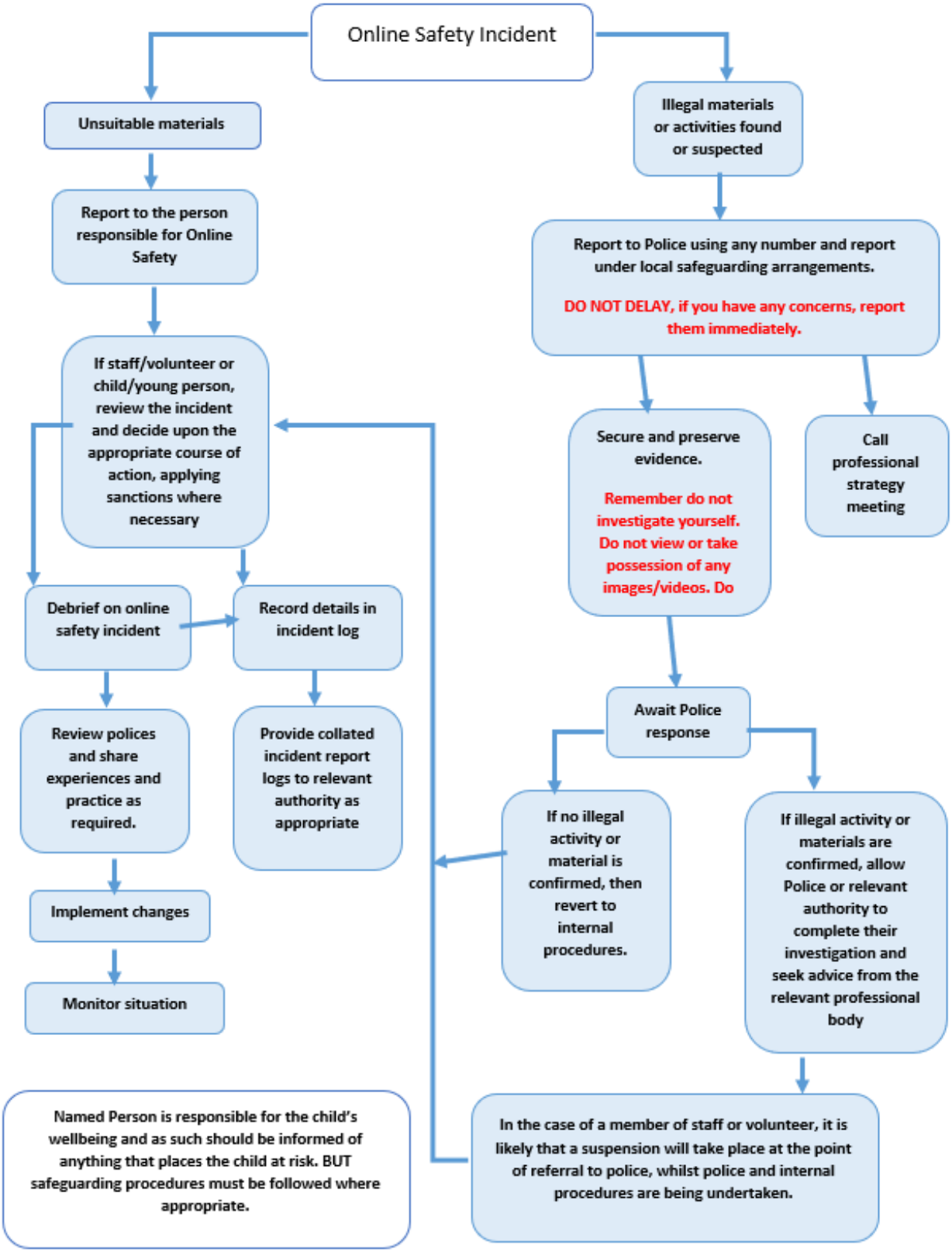
In the even of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action

E 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 potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

E Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix 1

Communication Technologies

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

Schools can complete the table choosing their own responses.

Communication Technologies	Staff & other adults				Students / Pupils			
	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 the school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking of photos on mobile phones / cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

Appendix 2

Dealing with unsuitable / inappropriate activities

2.1 – Usage restrictions form

Usage restrictions *The school should agree its own responses and complete / modify the pro forma as appropriate. This form may need to be duplicated to define the usage for staff and pupils*		Acceptable	Acceptable at certain times	Acceptable for nominated users	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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children					X
	Possession of an extreme pornographic image					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation)					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				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, website 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 (e.g. 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	
Online gaming (educational)						
Online gaming (non-educational)						
Online gambling						
Online shopping / commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting e.g. YouTube						

2.2 – Actions and sanctions form: Pupil incidents

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

2.3 – Actions and sanctions form: Staff incidents

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

Appendix 3

Sharing nudes and semi-nudes

How to respond to an incident – an overview for education settings

From Department for Digital, Culture, Media & Sport and UK Council for Internet Safety

In the latest advice for schools and colleges (UKCIS, 2020), the sharing of nudes and semi-nudes 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**.
- 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).

For further information, download the full guidance from:
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people (UKCIS, 2020)