All Saints' and St Richard's Church of England Primary School

All Saints and St Richards Primary School Online Safety Policy and Guidance for Education Settings

2017 - 2018

Policy Date	November 2017
Review Cycle	Annual
Review Date	September 2018

Contents

1. Creating an online safety ethos
    - 1.1. Aims and policy scope
    - 1.2. Writing and reviewing the online safety policy
    - 1.3. Key responsibilities of the community
        - 1.3.1. Key responsibilities of the management team
        - 1.3.2. Key responsibilities of the online safety/designated safeguarding lead (DSL)
        - 1.3.3. Key responsibilities of staff
        - 1.3.4. Additional responsibilities of staff managing the technical environment
        - 1.3.5. Key responsibilities of children and young people
        - 1.3.6. Key responsibilities of parents/carers
2. Online communication and safer use of technology
    - 2.1. Managing the website
    - 2.2. Publishing images online
    - 2.3. Managing email
    - 2.4. Official video conferencing and webcam use
    - 2.5. Appropriate safe classroom use of the internet and associated devices
    - 2.6. Management of school learning platforms/portals/gateways
3. Social media policy
    - 3.1. General social media use
    - 3.2. Official use of social media
    - 3.3. Staff personal use of social media
    - 3.4. Staff official use of social media
    - 3.5. Pupil use of social media
4. Use of personal devices and mobile phones
    - 4.1. Rationale regarding personal devices and mobile phones
    - 4.2. Expectations for safe use of personal devices and mobile phones
    - 4.3. Children use of personal devices and mobile phones
    - 4.4. Staff use of personal devices and mobile phones
    - 4.5. Visitors use of personal devices and mobile phones
5. Policy decisions

5.1. Recognising online risks

5.2. Internet use within the community

5.3. Authorising internet access

6. Engagement approaches

6.1. Engagement of children and young people

6.2. Engagement of children and young people who are considered to be vulnerable

6.3. Engagement of staff

6.4. Engagement of parents/carers

7. Managing information systems

7.1. Managing personal data online

7.2. Security and managing information systems

7.3. Filtering decisions

7.4. Management of applications to record progress

8. Responding to online incidents and concerns

Appendix A: Procedures for responding to specific online incidents or concerns (including 'sexting', online child sexual abuse and exploitation, indecent image of children, radicalisation and cyberbullying)

Appendix B: Questions to support DSLs responding to concerns relating to youth produced sexual imagery

Appendix C: Notes on the legal framework

Appendix D: Online safety contacts and references

1. Creating an Online Safety Ethos

1.1. Aims and policy scope

The purpose of *ASSR Primary School* online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that *ASSR Primary School* is a safe and secure environment.

- Safeguard and protect all members of *ASSR Primary School* community online.
- Raise awareness with all members of *ASSR Primary School* community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

✓ This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
✓ This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
✓ This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

- *ASSR Primary School* believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- *ASSR Primary School* identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- *ASSR Primary School* has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions.
- *ASSR Primary School* identifies that there is a clear duty to ensure that children are protected from potential harm online.

✓ *ASSR Primary School* online safety policy has been written by the school, involving staff and parents/carers, building on the East Sussex County Council (ESCC) online safety policy template, with specialist advice and input as required.
✓ The policy has been approved and agreed by the Leadership/Management Team and Governing Body
✓ The school has appointed the Designated Safeguarding Lead Gavin Davison, as an appropriate member of the leadership team and the online safety lead.
✓ The school has appointed a member of the Governing Body to take lead responsibility for online safety (e-Safety).
✓ The online safety (e–Safety) Policy and its implementation will be reviewed by the school/setting at least annually or sooner if required.

1.3 Key responsibilities of the community

All members of school/setting communities have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and also how to access and seek support and guidance.

1.3.1 The key responsibilities of the school/setting management and leadership team are:

- ✓ Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- ✓ Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- ✓ Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- ✓ Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- ✓ To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- ✓ To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- ✓ Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- ✓ Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- ✓ Making appropriate resources available to support the development of an online safety culture.
- ✓ Taking responsibility for online safety incidents and liaising with external agencies and support as appropriate.
- ✓ Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- ✓ Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- ✓ Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- ✓ To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- ✓ To ensure that the DSL works in partnership with the online safety e-Safety lead. (**if they are not the same person**)

1.3.2 The Key responsibilities of the Designated Safeguarding Lead (DSL) /online safety lead

The DSL is responsible for coordinating the whole school/setting online safety approaches, supporting and raising awareness with the wider community, promoting a safe and responsible online safety culture and acting as the lead for dealing with online safety issues that arise. The DSF responsibilities include:

- ✓ Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- ✓ Keeping up-to-date with current research, legislation and trends regarding online safety.

- ✓ Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- ✓ Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- ✓ Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- ✓ Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- ✓ Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- ✓ To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- ✓ Liaising with the local authority and other local and national bodies, as appropriate.
- ✓ Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other related procedures on a regular basis (at least annually) with stakeholder input.
- ✓ Ensuring that online safety is integrated with other appropriate school policies and procedures.
- ✓ Meet regularly with the governors/board/committee member with a lead responsibility for online safety

1.3.3 The key responsibilities for all members of staff are:

- ✓ Contributing to the development of online safety policies.
- ✓ Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- ✓ Taking responsibility for the security of school/setting systems and data.
- ✓ Having an awareness of a range of online safety issues and how they relate to the children in their care.
- ✓ Modelling good practice when using new and emerging technologies
- ✓ Embedding online safety education in curriculum delivery wherever possible.
- ✓ Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- ✓ Knowing when and how to escalate online safety issues, internally and externally.
- ✓ Being able to signpost to appropriate support available for online safety issues, internally and externally.
- ✓ Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- ✓ Demonstrating an emphasis on positive learning opportunities.
- ✓ Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- ✓ Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- ✓ Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- ✓ To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- ✓ Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- ✓ Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- ✓ Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.

- ✓ Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- ✓ Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- ✓ Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- ✓ Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- ✓ Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- ✓ Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 The key responsibilities of children and young people are:

- ✓ Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- ✓ Respecting the feelings and rights of others both on and offline.
- ✓ Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- ✓ Taking responsibility for keeping themselves and others safe online.
- ✓ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

1.3.6 The key responsibilities of parents and carers are:

- ✓ Reading the school/setting **Acceptable Use Policies**, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- ✓ Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- ✓ Role modelling safe and appropriate uses of technology and social media.
- ✓ Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- ✓ Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- ✓ Contributing to the development of the school/setting online safety policies.
- ✓ Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- ✓ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

Schools and settings will be using a variety of online communication and collaboration tools both informally and formally with children, parents/carers and staff. The following provide clear boundaries and expectations for safe use.

2.1 Managing the school/setting website

- ✓ The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

- ✓ The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.
- ✓ The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- ✓ The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- ✓ The administrator account for the school website will be safeguarded with an appropriately strong password.
- ✓ The school will post information about safeguarding, including online safety, on the school website for members of the community.

✓ *2.2 Publishing images and videos online*

- ✓ The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- ✓ The school/setting will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- ✓ In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- ✓ All members of staff are provided with a specific school/setting email address to use for any official communication.
- ✓ The use of personal email addresses by staff for any official school/setting business is not permitted.
- ✓ The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- ✓ Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- ✓ Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- ✓ Whole -class or group email addresses may be used for communication outside of the school (***in early years, infant and primary schools***).
- ✓ Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- ✓ School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use for educational purposes

Relevant for all settings who use video conferencing and webcams

- ✓ The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- ✓ All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- ✓ Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.

- ✓ School videoconferencing equipment will not be taken off school premises without permission.
- ✓ Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- ✓ Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- ✓ Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- ✓ Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- ✓ Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- ✓ When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- ✓ If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- ✓ The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet (and associated devices)

Relevant for all settings that provide internet access for children

- ✓ Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access curriculum policies for further information.
- ✓ The school/setting's internet access will be designed to enhance and extend education.
- ✓ Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- ✓ All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- ✓ Supervision of pupils will be appropriate to their age and ability
    - o At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - o At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

- ✓ All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- ✓ Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- ✓ The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- ✓ The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

3.0 *Social Media Policy*

3.1. General social media use

- ✓ Expectations regarding safe and responsible use of social media will apply to all members of ASSR Primary School community and exist in order to safeguard both the school/setting and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- ✓ All members of ASSR Primary School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- ✓ Information about safe and responsible use of social media will be communicated clearly and regularly to all members of ASSR Primary School community.
- ✓ All members of ASSR Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- ✓ The school's internet wi-fi access will not be used for personal social media and social networking sites whilst on the premises.
- ✓ Staff inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities.
- ✓ Any concerns regarding the online conduct of any member of ASSR Primary School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- ✓ Any breaches of school/setting policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, behaviour, safeguarding and child protection including the allegations against staff section.

3.2. Official use of social media

- ✓ Official use of social media sites by the school/setting will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement, education and promotion of school activities & curriculum.
- ✓ Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- ✓ Official school/setting social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- ✓ Staff will use school/setting provided email addresses to register for and manage any official approved social media channels.
- ✓ All communication on official social media platforms will be clear, transparent and open to scrutiny.

- ✓ Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- ✓ Official social media use will be in line with existing policies including anti-bullying and child protection and safeguarding.
- ✓ Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- ✓ Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- ✓ Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.
- ✓ Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- ✓ Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- ✓ Official social media channels will link back to the school/setting website and/or Acceptable Use Policy to demonstrate that the account is official.

3.3 Staff personal use of social media

- ✓ Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff meetings.
- ✓ Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school/setting **Acceptable Use Policy.**
- ✓ All communication between staff and members of the school community on school business will take place via official approved communication channels (***Official Twitter account, school website and office.)***
- ✓ Staff will not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.
- ✓ Any communication from pupils/parents received on personal social media accounts will be responded to by the designated safeguarding leads.
- ✓ Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites unless approved.
- ✓ All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- ✓ All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their personal social media use is compatible with their professional role and is in accordance with schools policies (**safeguarding and child protection, confidentiality, data protection etc**.) and the wider professional and legal framework.
- ✓ Members of staff who have access to the schools Social Media Networking sites are encouraged to manage and control the content they choose to share and post online. Only official users approved by the Head teacher/safeguarding officer of ASSR Primary School

may post in the capacity of the school. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

- ✓ Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- ✓ Members of staff are encouraged not to identify themselves as employees of ASSR Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/setting and also to safeguard the privacy of staff members and the wider community.
- ✓ Member of staff will ensure that they do not represent their personal views as that of the school/setting on social media.

✓ School/setting email addresses will not be used for setting up personal social media accounts.

3.4 Staff official use of social media

- ✓ Apply to members of staff that have been given access or have administration access to the schools official Social media accounts.

- ✓ If members of staff are participating in online activity as part of their capacity as an employee of the school/setting, then they are requested to be professional at all times and understand that they are an ambassador for the school/setting.
- ✓ Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- ✓ Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- ✓ Staff must ensure that any image identifying any student, staff member, parent or visitor posted on any official social media channel have appropriate consent.
- ✓ Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- ✓ Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the head teacher/manager of any concerns such as criticism or inappropriate content posted online.
- ✓ Staff using social media officially will sign the social media **Acceptable Use Policy.**

3.5 Pupils' use of social media

- ✓ Safe and responsible use of social media sites will be outlined for children and their parents as part of the **Acceptable Use Policy**.
- ✓ Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- ✓ Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- ✓ Any official social media activity involving pupils will be moderated by the school where possible.
- ✓ The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school or be responsible for the personal use or creation of Social Media accounts for children under this age.

- ✓ Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- ✓ Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

ASSR Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings and if used for taking pictures or sharing content online, should be in line with the appropriate safeguarding, social media or images policies.

4.2 Expectations for safe use of personal devices and mobile phones

- ✓ Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school/setting accepts no responsibility for the loss, theft or damage of such items. Nor will the school/setting accept responsibility for any adverse health effects caused by any such devices either potential or actual..
- ✓ All members of ASSR Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.
- ✓ School/setting mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies
- ✓ School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.4 Staff use of personal devices and mobile phones

- ✓ Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- ✓ Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- ✓ Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- ✓ Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- ✓ Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- ✓ If a member of staff breaches the school/setting policy then disciplinary action will be taken.
- ✓ If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- ✓ Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management section in the safeguarding and child protection policy.

4.5 Visitors' use of personal devices and mobile phones

- ✓ Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy whilst on school property.
- ✓ Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

5. Policy Decisions

. ASSR Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

- ✓ Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- ✓ The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. (**Schools should include appropriate details about the systems in place)**
- ✓ The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school/setting computer or device.
- ✓ Methods to identify, assess and minimise online risks will be reviewed regularly by the school leadership team.

5.2. Internet use throughout the wider school/setting community

- The school will liaise with local organisations to establish a common approach to online safety (e–Safety).
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

6. Engagement Approaches

6.1 Engagement and education of children and young people

- ✓ An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- ✓ Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.
- ✓ Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- ✓ Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- ✓ The school will reward positive use of technology by pupils.

.

6.2 Engagement and education of children and young people who are considered to be vulnerable

- ✓ ASSR Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- ✓ ASSR Primary School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff

- ✓ The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- ✓ Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular (at least annual) basis.
- ✓ All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- ✓ Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- ✓ The school/setting will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers

- ✓ ASSR Primary School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- ✓ Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.
- ✓ A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- ✓ Parents will be requested to read online safety information as part of the Home School Agreement.
- ✓ Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- ✓ Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- ✓ Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- ✓ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- ✓ Full information regarding the schools approach to data protection and information governance can be found in the schools information security policy.

7.2 Security and Management of Information Systems

Relevant for all settings who facilitate internet access

- ✓ devices must be proactively managed and secured with a minimum of WPA2 encryption.

- ✓ The security of the school information systems and users will be reviewed regularly.
- ✓ Virus protection will be updated regularly.
- ✓ Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- ✓ Files held on the school's network will be regularly checked.

7.3 Filtering Decisions

Relevant for all settings who facilitate internet access

All Schools subscribing to the East Sussex Education Network receive Smoothwall web filtering as standard as a part of the package. Smoothwall meets the requirements as outlined by the Safer Internet Centre for appropriate web filtering: (saferinternet.org.uk) Filtering Monitoring Smoothwall

- ✓ The governors/proprietors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- ✓ The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- ✓ All monitoring of school owned/provided systems will take place to safeguard members of the community.
- ✓ All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- ✓ The school uses educational filtered secure broadband connectivity through the East Sussex Education Network which is appropriate to the age and requirement of our pupils.
- ✓ The school uses Smoothwall filtering systems which block sites that fall into categories such as pornography, racial hatred, extremism, sites of an illegal nature, etc.
- ✓ The school will work with Schools ICT to ensure that filtering policy is continually reviewed.
- ✓ The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- ✓ If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- ✓ The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- ✓ Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.

- ✓ All changes to the school filtering policy will be logged and recorded.
- ✓ The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- ✓ Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, East Sussex Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

- ✓ The headteacher/manager is ultimately responsible for the security of any data or images held of children.
- ✓ Apps/systems which store personal data will be risk assessed prior to use.
- ✓ Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- ✓ Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- ✓ Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- ✓ Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Concerns

- ✓ All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- ✓ All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, cyberbullying, illegal content etc.
- ✓ The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- ✓ The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.
- ✓ Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- ✓ Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure
- ✓ Any complaint about staff misuse will be referred to the head teacher
- ✓ Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).
- ✓ Pupils, parents and staff will be informed of the schools complaints procedure.
- ✓ Staff will be informed of the whistleblowing procedure.
- ✓ All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- ✓ All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- ✓ The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- ✓ The school will inform parents/carers of any incidents of concerns as and when required.
- ✓ After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

- ✓ Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the SLES Safeguarding Team or East Sussex Police via 101 or 999 if there is immediate danger or risk of harm.
- ✓ The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to East Sussex Police.
- ✓ If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the SLES Safeguarding Team.
- ✓ If an incident of concern needs to be passed beyond the school then the concern will be escalated to the SLES Safeguarding Team to communicate to other schools/settings in East Sussex.
- ✓ Parents and children will need to work in partnership with the school to resolve issues.

8.1. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- ✓ ASSR Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- ✓ If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead should obtain advice immediately through SPOA or Sussex Police.
- ✓ If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Pan Sussex Child Protection and Safeguarding Procedures
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform East Sussex police via 101 (using 999 if a child is at immediate risk)
- ✓ The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- ✓ The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

8.2 Responding to concerns regarding Indecent Images of Children (IIOC)

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet otherwise known as 'downloading'. More information about these offences can be found within the legal framework section.

- ✓ ASSR Primary School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- ✓ The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- ✓ The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- ✓ If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through SPOA and/or Sussex Police.

- If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Pan-Sussex Child Protection and Safeguarding procedures.
    - Immediately notify the school Designated Safeguard Lead.

- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), East Sussex police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via IWF .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via IWF .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform Sussex police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

8.3. Responding to concerns regarding radicalisation and extremism online

Useful links regarding online hate, radicalisation and extremism

DfE: www.educateagainsthate.com
Report online hate and terrorism: www.gov.uk/report-terrorism:
NCALT e-learning http://course.ncalt.com/Channel_General_Awareness/01/index.html
National helpline: 020 7340 7264 Counter.extremism@education.gsi.gov.uk

- ✓ The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils
- ✓ Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the SLES Safeguarding Team and/or East Sussex Police.

8.4 Responding to concerns regarding cyberbullying

- ✓ Cyberbullying, along with all other forms of bullying, of any member of ASSR Primary School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

- ✓ All incidents of online bullying reported will be recorded.
- ✓ There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- ✓ If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through Sussex Police.
- ✓ Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- ✓ The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- ✓ Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- ✓ Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Appendix C

Notes on the Legal Framework

Many young people and indeed some staff and adults use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It must not replace professional advice and schools and settings should always consult with the Local Authority Designated Officer if there is a conduct issue as per the guidance and flowchart issued in July 2016. Contact should be made with the Single Point of Advice and Sussex Police if they are concerned that an offence may have been committed.

Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet and this list is not exhaustive.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a "higher law" which affects all other laws. Within an education context, human rights for schools and settings to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination

- The right to education

These rights are not absolute. Schools and settings are obliged to respect these rights and freedoms, balancing them against rights, duties and obligations, which may arise from other relevant legislation.

Data protection and Computer Misuse

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film, video and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, organisations have to follow a number of set procedures.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

The Protection of Freedoms Act 2012

This act requires schools to seek permission from a parent / carer to use Biometric systems.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Obscene and Offensive Content, Hate and Harassment

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence and this includes electronic transmission. For the purposes of the Act an article is deemed to be obscene if its effect is to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the content. This offence can result in imprisonment for up to 5 years.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This offence can result in imprisonment for up to 2 years.

Protection from Harassment Act 1997

This Act is relevant for incidents that have happened repeatedly (i.e. on more than two occasions). The Protection from Harassment Act 1997 makes it a criminal and civil offence to pursue a course of conduct which causes alarm and distress, which includes the publication of words, which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The victim can also bring a civil claim for damages and an injunction against the abuser, although in reality this is a remedy that is only used by individuals with the financial means to litigate, and only possible if the abuser can be identified, which is not always straightforward.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

The Protection of Freedoms Act 2012 (2A and 4A) and Serious Crimes Act 2015 (section 76) - Stalking and Harassment

The Protection of Freedoms Act 2012 was updated in 2015 and two sections were added regarding online stalking and harassment, section 2A and 4A. Section 2A makes it offence for a perpetrator to pursue a course of conduct (2 or more incidents) described as "stalking behaviour" which amounts to harassment. Stalking behaviours include following, contacting/attempting to contact, publishing statements or material about the victim, monitoring the victim (including online), loitering in a public or private place, interfering with property, watching or spying. The Serious Crime Act 2015 Section 76 also created a new offence of controlling or coercive behaviour in intimate or familial relationships which will include online behaviour.

Criminal Justice and Courts Bill 2015 (section 33) - Revenge Pornography

Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress, often referred to as "revenge porn". The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years.

Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an offence under the Protection from Harassment Act 1997. This law and the term "revenge porn" only applies to images or videos of those over 18. For more information access: Revenge Porn Helpline

Libel and Privacy Law

These matters will be dealt with under civil rather than criminal law.

Libel is defined as 'defamation by written or printed words, pictures, or in any form other than by spoken words or gestures' and as such could the author could be held accountable under Defamation law which was created to protect individuals or organisations from unwarranted, mistaken or untruthful attacks on their reputation. Defamation is a civil “common law” tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.

A civil action for defamation can be brought by an individual or a company, but not by a public authority. Where defamatory material is posted on a website, the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

If social media is used to publish private and confidential information (for example breaches of data protection act) about an individual, then this could give rise to a potential privacy claim and it is possible for individuals to seek an injunction and damages.

Education Law

Education and Inspections Act 2006

Section 89 of the states that every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents. This act (89.5) gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

The Education Act 2011

Section 13 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance of not publishing named allegations against teachers online as this can lead to prosecution. Schools should contact the LADO team for advice.

Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. This act gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. The DfE advice on these sections of the Education Act 2011 can be found in the document: “Screening, searching and confiscation – Advice for head teachers, staff and governing bodies”
www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The School Information Regulations 2012

This act requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Sexual Offences

Sexual Offences Act 2003

There are many offences under the Sexual Offence Act 2003 which can be related to or involve the misuse of technology. This includes (but is not limited to) the following points.

Section 15 - Meeting a child following sexual grooming. The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world with the intention of committing a sexual offence. This offence can result in imprisonment for up to 10 years.

Causing or inciting a child under 16 to watch or take part in a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

- **Section 8. Causing or inciting a child under 13 to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 9. Sexual Activity with a child** (Can result in imprisonment for up to 14 years)
- **Section 10. Causing or inciting a child (13 to 16) to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 11. Engaging in sexual activity in the presence of a child** (Can result in imprisonment for up to 14 years)
- **Section 12. Causing a child to watch a sexual act** (Can result in imprisonment for up to 10 years)
- **Section 13. Child sex offences committed by children (offender is under 18)** (Can result in imprisonment for up to 5 years)

Section 16 - Abuse of position of trust: sexual activity with a child.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they know as a result of being in their professional role. It is also an offence cause or incite a child with whom they are in a position of trust to engage in sexual activity, to engage in sexual activity in the presence of a child with whom they are in a position of trust, or cause a child with whom they are in a position of trust to watch a sexual act. Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust and this can result in imprisonment for up to 5 years.

Indecent Images of Children

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom under two pieces of legislation; **Criminal Justice Act 1988**, section 160 and **Protection of Children Act 1978**, section 1.1.a. Indecent images of children are images of children (under 18 years) depicting sexual posing, performing sexual acts on themselves or others, animals or sadomachisism.

A child for these purposes is considered to be anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This offence can include images taken by and distributed by the child themselves (often referred to as “Sexting”, see section 9.1). Viewing an indecent image of a child on your computer or phone means that you have made a digital image and printing/forwarding/sharing/publishing can be considered to be distribution. A person convicted of such an offence may face up to 10 years in prison.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess “extreme pornographic images”. 63 (6) identifies that such images must be considered to be “grossly offensive, disgusting or otherwise obscene”. Section 63 (7) includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a

corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.

The Serious Crime Act 2015

Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communications. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment.

Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment.

This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation.

Appendix D

Online Safety (e-Safety) Contacts and References

East Sussex Support and Guidance:

If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on: 01323 464222 or **0-19.SPOA@eastsussex.gov.uk**

If you think the child is in immediate danger, you should call the police on 999.

Sussex Police: (for non-urgent Police contact) 101 or 01273 470101

Standards and Learning Effectiveness Service (SLES): Support and Intervention Manager: Safeguarding Victoria Stutt Victoria.stutt@eastsussex.gov.uk

East Sussex Schools ICT Service: Richard May Richard.may@eastsussex.gov.uk

Local Authority Designated Officer: Amanda Glover Amanda.glover@eastsussex.gov.uk

East Sussex Safeguarding Children Board (LSCB): 01273 481544 or lscbcontact@eastsussex.gov.uk

National Links and Resources:

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Lucy Faithfull Foundation: www.lucyfaithfull.org

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/