Bexhill Academy Online Safety Policy

Updated: March 2019

Next Review: March 2020

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

Bexhill Academy 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.

Bexhill Academy 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.

Bexhill Academy 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.

Bexhill Academy identifies that there is a clear duty to ensure that children are protected from potential harm online.

The purpose of Bexhill Academy's 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 of technology to ensure that Bexhill Academy is a safe and secure environment.
- Safeguard and protect all members of the Bexhill Academy community online.
- Raise awareness with all members of the Bexhill Academy 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 (whilst working for the Academy) , volunteers and other individuals who work for or provide services on behalf of the academy (collectively referred to as ‘staff‘ in this policy)
- visitors to the academy
- students

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 academy 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 academy policies including (but not limited to) Safeguarding and Child protection, Friendship and Anti-bullying, Engagement for Learning Policy, Acceptable Use Policies, Confidentiality Policy, Searching and Confiscation guidance and relevant curriculum policies including computing, Personal Social and Health Education (PSHE) and Sex and Relationships Education (SRE).

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is Trudy Hillman

The Academy Online Safety Lead is Steve Blake.

Policy approved by Principal   ……………SARA ATTWOOD………………………………… Date: ……30.3.19………

Policy approved by Academy Trust Board: …………………………………………….. Date: ……31.3.19………

The date for the next policy review is March 2020

> Bexhill Academy online safety policy has been written by the school, involving staff, pupils 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 Senior Leadership Team and Academy Trust Board.
>
> The academy has appointed the Designated Safeguarding Lead, Trudy Hillman, as an appropriate member of the leadership team and the online safety lead.
>
> The school has appointed Sara Attwood, Safeguarding Governor, as the member of the Academy Trust Board to take lead responsibility for online safety (e-Safety).
>
> The online safety (e–Safety) Policy and its implementation will be reviewed by the academy 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 Key responsibilities of the Senior Leadership Team

The leadership team (including the Academy Trust Board) within Bexhill Academy have statutory responsibilities for child protection, of which online safety is an essential element. KCSiE 2016 highlights a range of specific statutory responsibilities for schools and colleges regarding online safety which governing bodies and proprietors need to be aware of within part two: the management of safeguarding. This includes ensuring that appropriate filtering and monitoring of internet access is in place, that all members of staff receive appropriate training and guidance and that the curriculum prepares children for the digital world.

Additional guidance regarding online safety is provided to schools and colleges within Annex C of KCSiE 2016.

1.3.1 The key responsibilities of the Academy 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 academy community.

Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.

Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.

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 academy community whilst ensuring children have access to required educational material.

To work with and support technical staff in monitoring the safety and security of academy systems and networks and to ensure that the academy 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 academy 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 academy community to access regarding online safety concerns, including internal, local and national support.

To ensure a member of the Academy Trust Board is identified with a lead responsibility for supporting online safety. This will be Sara Attwood as the Safeguarding Lead on the Trust Board.

To ensure that the DSL works in partnership with the online safety lead.

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

The key responsibilities of the Designated Safeguarding Lead are:

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.

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 Senior Leadership Team, Academy Trust Board 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 board member with a lead responsibility for online safety

1.3.3 Key responsibilities of staff

All members of staff play an essential role in creating a safe culture within settings, both on and offline. All members of staff should seek to promote safe and responsible online conduct with and by children as part of the curriculum and as part of their safeguarding responsibilities. All members of staff will need to role model positive behaviours when using technologies, either directly with children or in the wider context. All staff should be aware of and ensure they adhere to the Acceptable Use Policies (AUPs).

Where services are provided within schools/settings by external contractors, it is essential that the school takes steps to ensure that outside providers support the schools online safety ethos and will adhere to the settings online safety policy and practices.

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 academy 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. Additional responsibilities for staff managing the technical environment

Members of staff who are responsible for managing the school/setting technical environment have an essential role to play in establishing and maintaining a safe online environment and culture within establishments.

Technical staff will need clear supervision and support in their roles by the leadership and management team (including safeguarding leads) and, along with all staff, will require regular training and professional opportunities to enable them to remain up-to-date with emerging online safety issues.

Technical staff should be clear about the procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the DSL and/or Principal in line with existing academy safeguarding policies (including allegations and whistleblowing).

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 academy's 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 academy's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL and Pastoral Teams.

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 academy’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 Key responsibilities of children and young people

The essential role and responsibilities for children and young people themselves in relation to their own online safety should not be underestimated. Children should be encouraged and empowered to develop safe and responsible online behaviours over time which will enable them to manage and respond to online risks as they occur.

It should also be understood that children are more likely to be aware of and understand new developments within technology and may be able to provide schools and settings with an excellent way of keeping up-to-date with the rapidly changing pace of development, especially within social media and the associated apps and games.

The key responsibilities of children and young people are:

Contributing to the development of online safety policies.

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.

Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6. Key responsibilities of parents and carers

Parents /carers play a crucial role in developing children's safe and responsible online behaviours, especially where a majority of children's access will be taking place when they are not on the school/setting site. Schools have a clear responsibility to work in partnership with families to raise awareness of online safety issues. Through this approach, parents/carers can help schools/settings to reinforce online safety messages and promote and encourage safe online behaviours wherever, and whenever, children use technology.

The key responsibilities of parents and carers are:

Reading the 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 academy’s online safety policies.

Using school systems, such as Show My Homework, 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

Bexhill Academy will be using a variety of online communication and collaboration tools both informally and formally with children, parents/carers and staff. It will be important that managers and leaders are aware of this use and provide clear boundaries and expectations for safe use.

2.1 Managing the school/setting website

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

The Principal will take overall editorial responsibility for online content published by the academy and will ensure that content published is accurate and appropriate.

The academy 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 academy website will be safeguarded with an appropriately strong password.

The academy will post information about safeguarding, including online safety, on the academy website for members of the community.

2.2 Publishing images and videos online

The academy will ensure that all images and videos shared online are used in accordance with the Use of Images procedures.

The academy will ensure that all use of images and videos take place in accordance other policies and procedures including Acceptable Use Policies, Codes of Conduct, Social Media etc

In line with the academy procedures, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

Pupils may only use academy provided email accounts for educational purposes

All members of staff are provided with a specific email address to use for any official communication.

The use of personal email addresses by staff for any official academy business is not permitted.

The forwarding of any chain messages/emails etc. is not permitted.

Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the academy safeguarding files/records.

Academy 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

The academy 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.

Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.

External IP addresses will not be made available to other sites.

Videoconferencing contact details will not be posted publically.

Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.

Academy videoconferencing equipment will not be taken off academy premises without permission.

Staff will ensure that external video conference 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

Pupils will ask permission from a teacher before making or answering a video conference call or message.

Video conferencing will be supervised appropriately for the pupils' age and ability.

Parents and carers consent will be obtained prior to children taking part in video conferencing 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 video conferencing administration areas or remote control pages.

Unique log on and password details for the educational video conferencing services will only be issued to members of staff and kept secure.

Content

When recording a video conference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of video conference 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 academy will check that recording is acceptable to avoid infringing the third party intellectual property rights.
-
- The academy will establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site the academy 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)

Increased use of internet enabled devices and improved Internet access and its impact on pupils learning outcomes must be considered by leaders and managers. Developing safe and effective practice in using the Internet for teaching and learning is essential.

All members of staff must be aware that no search engine or filtering tools is ever completely safe and appropriate supervision, use of safe search tools (where possible), pre-checks of search terms, age appropriate education for pupils and robust classroom management must always be in place. However, despite these steps children may still be exposed to inappropriate content therefore leaders must ensure that there are clear procedures for reporting access to unsuitable content, which are known by both children and staff.

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read and a whole curriculum approach may be required. Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for pupils to develop skills in evaluating Internet content, for example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of. Additionally, the potential risk of exposure to extremist content when researching some content must also be considered.

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 academy’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.

All pupils will be appropriately supervised when using technology, according to their ability and understanding.

All academy owned devices will be used in accordance with the Acceptable Use Policy and with appropriate safety and security measures 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 academy will use age appropriate search tools as decided by the academy following an informed risk assessment to identify which tool best suits the needs of our community.

The academy will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The academy will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of Academy learning platforms/portals/gateways

Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.

Pupils/staff will be advised about acceptable conduct and use when using the LP.

Only members of the current pupil, parent/carers and staff community will have access to the LP.

All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of leadership before reinstatement.
e) A pupil’s parent/carer may be informed.

A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.

Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

Expectations regarding safe and responsible use of social media will apply to all members of the Bexhill Academy community and exist in order to safeguard both the academy 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 the Bexhill Academy 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 the Bexhill Academy community.

All members of the Bexhill Academy 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 academy will control pupil and staff access to social media and social networking sites whilst on site and using academy provided devices and systems

The use of social networking applications during academy hours for personal use is not permitted,

Inappropriate or excessive use of social media during academy/work hours or whilst using academy/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 the Bexhill Academy community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as Friendship and Anti Bullying, Managing Allegations against staff, Engagement for Learning, Safeguarding and Child Protection.

Any breaches of academy 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 Friendship and Anti-bullying, Engagement for Learning, safeguarding and child protection including the allegations against staff section.

3.2. *Official use of social media*

Bexhill Academy official social media channels are: Twitter/Facebook

Official use of social media sites by the academy will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

Official academy social media channels will be set up as distinct and dedicated social media sites for educational or engagement purposes.

Staff will use academy provided email addresses to register for and manage any official approved social media channels.

Members of staff running official social media channels will read the Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.

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 Friendship and 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 procedures.

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 academy 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.

Public communications on behalf of the academy will, where possible, be read and agreed by at least one other colleague.

Official social media channels will link back to the academy website and/or Acceptable Use Policy to demonstrate that the account is official.

The academy will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

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 training opportunities.

All members of staff are advised not to communicate with or add as ‘friends’ any current or past children/pupils or current or past pupils’ family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or a member of the Leadership Team.

If on-going contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.

All communication between staff and members of the school community on school business will take place via official approved communication channels.

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 Principal/manager.

Any communication from pupils/parents received on personal social media accounts will be reported to the designated safeguarding lead.

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.

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 social media use is compatible with their professional role and is in accordance with the academy's policies and the wider professional and legal framework.

Members of staff will be encouraged to manage and control the content they share and post online. 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 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 academy.

Members of staff are encouraged not to identify themselves as employees of Bexhill Academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the academy and also to safeguard the privacy of staff members and the wider community.

Members of staff will ensure that they do not represent their personal views as that of the academy on social media.

Academy email addresses will not be used for setting up personal social media accounts.

Members of staff who follow/like the academy's social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

3.4 *Staff official use of social media*

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 that they are an ambassador for the academy.

Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the academy.

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 posted on any official social media channel have appropriate written parental consent.

Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the academy unless they are authorised to do so.

Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and the Principal of any concerns such as criticism or inappropriate content posted online.

Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

Staff using social media officially will sign the Acceptable Use Policy.

3.5 Pupils' use of social media

Social media is now an everyday form of communication for many children and young and forms a vital part of growing up in today's modern Britain and the wider global society.

Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

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.

Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles privacy protected.

Any official social media activity involving pupils will be moderated by the school where possible.

The academy is aware that many popular social media sites state that they are not for children under the age of 13, therefore the academy will not create accounts within school specifically 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 academy policies including the Friendship and Anti-bullying and Engagement for Learning

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

Mobile phones and other personal devices such as tablets, smart watches, e-readers, electronic dictionaries, digital cameras and laptops are considered to be an everyday item in today's society and even children in early years settings may own and use online personal devices regularly. Mobile phones and personal devices can be used to communicate in a variety of ways with texting, cameras, voice recording and internet accesses all common features.

However, mobile phones and personal devices can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render children or staff subject to online (cyber)bullying;
- Internet access on phones and personal devices can allow children and adults to bypass security settings and filtering;
- They can undermine classroom discipline as they can be used on "silent" mode;
- If used to access school data then they can breach data protection and confidentiallity policies;
- Mobile phones and devices with integrated cameras and other recording systems could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of children or staff.

4.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the Bexhill Academy community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by Bexhill Academy and is covered in appropriate policies including the school Acceptable Use Policy and Engagement for Learning Policy

Bexhill Academy recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

4.2 Expectations for safe use of personal devices and mobile phones

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies

Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The academy accepts no responsibility for the loss, theft or damage of such items. Nor will the academy accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Mobile phones and personal devices are not permitted to be used inside the academy building during the academy day

.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Engagement for learning and Friendship and anti-Bullying Policy.

Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.

All members of Bexhill Academy community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

All members of Bexhill Academy community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

All members of Bexhill Academy 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 academy policies.

Academy mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.

4.3 Pupils use of personal devices and mobile phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.

All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.

Pupil’s personal mobile phones and personal devices will be kept switched off and kept out of sight in the building during the academy day.

Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

If a pupil needs to contact his/her parents/carers they will be allowed to use an academy phone.

Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Principal.

Pupils should protect their phone numbers by only giving them to trusted friends and family members.

Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil’s withdrawal from either that examination or all examinations.

If a pupil breaches the academy policy then the phone or device will be confiscated and will be held in a secure place.

Academy staff may confiscate a pupil’s mobile phone or device if they believe it is being used to contravene the academy’s Engagement for Learning or Friendship and Anti-Bullying policy. Searches of mobile phone or personal devices will be carried out in accordance with the academy’s policy. If there is suspicion that material on a pupil’s personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

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. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

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 academy policy and procedures e.g. confidentiality, Acceptable Use etc.

Staff personal mobile phones and devices will be switched off/switched to ‘silent’ mode during lesson times.

Bluetooth or other forms of communication should be “hidden” or switched off during lesson times.

Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.

Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.

If a member of staff breaches the academy 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 academy 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 academy acceptable use policy.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

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

The academy will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.

The academy 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 an academy computer or device.

Methods to identify, assess and minimise online risks will be reviewed regularly by the leadership team.

5.2. Internet use throughout the wider academy community

The academy will liaise with local organisations to establish a common approach to online safety (e–Safety).

The academy 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 academy's computer system or internet on site

5.3 *Authorising internet access*

The academy will maintain a current record of all staff and pupils who are granted access to the academy's devices and systems.

All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any academy resources.

Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

When considering access for vulnerable members of the community (such as with children with special education needs) the academy will make decisions based on the specific needs and understanding of the pupil(s).

6. *Engagement Approaches*

6.1 *Engagement and education of children and young people*

Online safety forms an important part of the Computing curriculum programmes of study for children within schools and this highlights the importance for children to use technology safely and respectfully, understand how to keep personal information private and be able identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies from an increasingly early age. Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Critical awareness of the dangers and consequences of plagiarism, copyright, piracy, reliability and bias will need to be explored. Children will need to develop an understanding on how to become safe and responsible online or digital citizens and this should be developed within an appropriate Personal Social and Health Education (PSHE) curriculum.

An online safety (e-Safety) curriculum will be established and embedded throughout the whole academy, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

Education about safe and responsible use will precede internet access.

Pupils’ input will be sought when writing and developing academy online safety policies and practices, including curriculum development and implementation.

Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.

All users will be informed that network and Internet use will be monitored.

Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

External support will be used to complement and support the academy’s internal online safety (e-Safety) education approaches.

The academy will implement peer education to develop online safety as appropriate to the needs of the pupils.

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

Bexhill Academy is aware that some children may be considered to be more vulnerable online due to a range of factors.

Bexhill Academy 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.

Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.

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 academy 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

Bexhill Academy 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 academy online safety (e-Safety) policy and expectations in newsletters, letters, the prospectus and on the website.

A partnership approach to online safety at home and at school with parents will be encouraged.

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.

7.2 Security and Management of Information Systems

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless 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.

- Portable media may not be used without specific permission followed by an anti-virus /malware scan.

- Unapproved software will not be allowed in work areas or attached to email.

- Files held on the school's network will be regularly checked.

- The network manager will review system capacity regularly.

- The appropriate use of user logins and passwords to access the school network will be enforced for all users.

- All users will be expected to log off or lock their screens/devices if systems are unattended.

- The school will log and record internet use on all school owned devices

Password policy

All users will be informed not to share passwords or information with others and not to login as another user at any time.

- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff and pupils to change their passwords every term.

7.3 Filtering Decisions

- The Trust Board will ensure that the academy has age and ability appropriate filtering and monitoring in place whilst using academy devices and systems to limit children's exposure to online risks.

- The academy'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 academy owned/provided systems will take place to safeguard members of the community.

- All users will be informed that use of academy systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

- The academy uses educational filtered secure broadband connectivity through the East Sussex Education Network which is appropriate to the age and requirement of our pupils.

- The academy uses Smoothwall filtering systems which block sites that fall into categories such as pornography, racial hatred, extremism, sites of an illegal nature, etc.

- The academy will work with Schools ICT to ensure that filtering policy is continually reviewed.

- The academy will have a clear procedure for reporting breaches of filtering which all members of the academy 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 ICT Team and will then be recorded and escalated as appropriate.

- The academy filtering system will block all sites on the Internet Watch Foundation (IWF) list.

- Requests for changes to the academy filtering policy will be referred to the ICT HelpDesk. The request will be risk assessed by the Head of Department with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.

- All changes to the academy filtering policy will be logged and recorded via the ICT HelpDesk.

- 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 academy 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 Principal 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 academy 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 password protected if taken off site. All loss or theft must be reported to the ICT Help Desk and the leadership team immediately.

- 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 academy's 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

Relevant for all settings

Guidance:

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used.

Online Safety (e-Safety) risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Potential concerns can often be dealt with at a personal level by ensuring children are able to identify and speak with a trusted adult. Bexhill Academy will ensure that all children know how to respond if they encounter unsuitable material online, for example placing a tablet screen down, closing a laptop lid, minimising a webpage or turning the screen off (not closing the page as that means the member of staff can access and report the content if required) and immediately telling a member of staff. Teachers and other members of staff are the first line of defence; their observation of classroom behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff must also be vigilant about other member of staffs' behaviour on and offline and reporting any concerns noticed should be encouraged to develop a safe culture.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, Bexhill Academy will determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with. If Bexhill Academy is unsure about how to respond to online safety concerns then they should consult with the SLES Safeguarding Team.

Safeguarding concerns and incidents should be reported to Single Point of Access, in line with East Sussex Safeguarding and Child Protection model policy.

- 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 Bexhill Academy will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, cyber bullying, 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 Academy's complaints procedure.

- Complaints about online bullying will be dealt with under the Academy's Friendship and Anti-bullying policy and procedure

- Any complaint about staff misuse will be referred to the Principal

- 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 academy's complaints procedure.

- Staff will be informed of the whistleblowing procedure.

- All members of the Bexhill Academy will need to be aware of the importance of confidentiality and the need to follow the official academy procedures for reporting concerns.

- All members of Bexhill Academy 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 academy community.

- The academy will manage online safety (e-Safety) incidents in accordance with the academy discipline/behaviour policy where appropriate.

- The academy will inform parents/carers of any incidents of concerns as and when required.

- After any investigations are completed, the academy 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 academy 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 academy 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 academy 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 academy to resolve issues.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

Youth Produced Sexual Imagery or "Sexting" can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website.

Children and young people will always look to push the boundaries, especially when they go through puberty and are an age where they are more sexually and socially aware. Children typically do not use the term "sexting", usually referring to the images as "selfies" and may decide to send such pictures or videos for many reasons. For younger children (early years and primary school aged) indecent images or videos may be taken or shared out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyber bullying, sexual exploration, impulsive behaviour or even exploitation due to blackmail from a friend, partner, or other on or offline contact. There can also be emotional and reputation damage that can come from having intimate photos forwarded to others or shared online including isolation, bullying, low self-esteem, loss of control, creating of a negative "digital footprint" or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation.

Whilst is it important for professionals not to condone the creation of youth produced sexual imagery it is important to recognise that many young people (and indeed adults) view sharing sexual images as part of a “normal” relationship in today’s modern society.

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age, fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (this includes downloading or opening an image that has been sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with consent. “Sexts” may be viewed as police evidence and it is essential that Bexhill Academy secures devices and seeks advice immediately when dealing with concerns.

It should be noted that prosecution of children for sharing indecent images for a first offence is rare. The decision to criminalise children and young people for sending sexualised images will need to be considered and made on a case by case basis based on a number of factors including age, intent and vulnerability of children involved.

‘Keeping Children Safe in Education’ 2016 highlights the need for all members of staff to be aware that abuse can be perpetrated by children themselves, including sexting, and there is a need for all members of staff to be aware of concerning behaviour and appropriate safeguarding responses.

It is essential that Bexhill Academy handles ‘sexting’ incidents as carefully as possible and offer support to all parties involved whilst abiding by the law and also do not compromise police investigations.

Should an incident arise which necessitates criminal investigation then it may require the seizure of the phone/device and any other devices involved or identified as potentially having access to the imagery.

- Bexhill Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as “sexting”).
- The academy will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Bexhill Academy views “sexting” as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The academy will follow the guidance as set out in the non-statutory UKCCIS advice ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’.
- If the academy are made aware of incident involving indecent images of a child the academy will:
    - Act in accordance with the academy’s child protection and safeguarding policy and the relevant East Sussex Local Safeguarding Children Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
    - Make a referral to children’s social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.

- Inform parents/carers about the incident and how it is being managed.
- Implement appropriate sanctions in accordance with the academy's behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The academy will not view an image suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The academy will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the academy network or devices then the academy will take action to block access to all users and isolate the image.
- The academy will need to involve or consult the police if images are considered to be illegal.
- The academy will take action regarding indecent images, regardless of the use of academy equipment or personal equipment, both on and off the premises.
- The academy will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

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

Guidance:

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or exploited via the use of technology and the internet. Typically this is referred to as "online grooming" however this term can sometimes be considered to be too narrow when considering online child sexual abuse as using the term “grooming” may imply that the behaviour has taken place over a period of time whilst an offender has built a relationship and gained the trust of their victim. Whilst this longer term process still occurs, current trends identified nationally (CEOP/NCA) and locally would suggest that the period of engagement between offender and victim can in many cases be extremely brief. In 2015, CEOP identified that the objectives of online child sexual abuse have evolved and can lead to a range of offending outcomes, such as deceiving children into producing indecent images of themselves or engaging in sexual chat or sexual activity over webcam. Online child sexual abuse can also result in offline offending such as meetings between an adult and a child for sexual purposes following online engagement.

OSCE can also be perpetrated by young people themselves and these issues should be viewed and responded to in line with the East Sussex Local Safeguarding Children Board procedures.

- Bexhill Academy will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The academy will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Bexhill Academy 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 academy 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 academy is made aware of an incident involving online child sexual abuse of a child then the academy will:
    - Act in accordance with the academy’s 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)
    - Where appropriate the academy will involve and empower children to report concerns regarding online child sexual abuse eg by using the Click CEOP report form: CEOP Safety Centre
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the academy is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The academy will take action regarding online child sexual abuse regardless of the use of academy equipment or personal equipment, both on and off the academy premises.
- The academy will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the academy will seek support from SPOA to enable other schools to take appropriate action to safeguard their community.
- The academy will ensure that the Click CEOP report button link is visible on the school website and available to pupils and other members of the academy community

9.3. 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'.

- Bexhill Academy 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 academy will take action regarding the Indecent Images of Children (IIOC) regardless of the use of academy equipment or personal equipment, both on and off the premises.
- The academy will take action to prevent accidental access 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 academy 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 academy is made aware of Indecent Images of Children (IIOC) then the academy will:
  - Act in accordance with the academy's child protection and safeguarding policy and the relevant Pan-Sussex Child Protection and Safeguarding procedures.
  - Immediately notify the 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 academy is 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 academy 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 academy are made aware that indecent images of children have been found on the academy's electronic devices then the academy 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 academy is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the academy, then the academy will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the 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 academy's Safeguarding Policy.

  - Follow the appropriate academy policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

From 1st July 2015 specified authorities, including all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015(“the CTSA 2015”), in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism” This duty is known as the Prevent duty. The statutory Prevent guidance summarises the requirements on schools as undertaking risk assessment, working in partnership, staff training and IT policies.

Academy Safeguarding Staff understand when it is appropriate to make a referral to the Channel programme using the Prevent Referral form (available on Czone at: https://czone.eastsussex.gov.uk/supportingchildren/equality/Documents/Prevent School Toolkit 2015.docx). Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual’s engagement with the programme is entirely voluntary at all stages.

- The academy will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in the academy and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the academy safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing academy policies, including Friendship and Anti-bullying, Engagement for Learning etc. If the academy 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.

9.5. *Responding to concerns regarding cyber bullying*

Online or cyber bullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

Cyber bullying is becoming increasingly prevalent with the rapid advances and use of modern technology. Mobile, internet and wireless technologies have increased the pace of communication and brought significant benefits to users worldwide but their popularity provides increasing opportunity for misuse through 'cyber bullying', with worrying consequences. It's crucial that children and young people as well as adults, use their devices and the internet safely and positively and they are aware of the consequences of misuse. As technology develops, bullying techniques can evolve to exploit it.

- Cyber bullying, along with all other forms of bullying, of any member of the Bexhill Academy community will not be tolerated. Full details are set out in the academy 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 academy community affected by online bullying.
- If the academy 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 academy 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 academy to support the approach to cyber bullying and the academy's e-Safety ethos.
    -

- Sanctions for those involved in online or cyber bullying 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 academy for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the academy's Friendship and 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.

9.6. *Responding to concerns regarding online hate*

Guidance:

There are some situations whereby posting offensive content online may be viewed as illegal as either harassment or possibly as a hate crime. Hate crimes are any crimes that are targeted at a person because of hostility or prejudice towards that person's:

- disability
- race or ethnicity
- religion or belief
- sexual orientation
- transgender identity

- Online hate at Bexhill Academy will not be tolerated. Further details are set out in the academy policies regarding anti-bullying and behaviour

- All incidents of online hate reported to the academy will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant academy policies and procedures
- The Police will be contacted if a criminal offence is suspected. If the academy is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Sussex Police.

Appendix B

Questions to support DSLs responding to concerns relating to youth produced sexual imagery

The following statements may DSLs to consider how best to respond to concerns relating to youth produced sexual imagery:

Child/Young person involved

- What is the age of the child(ren) involved?
    - If under 13 then a consultation/referral to Children's Social Care should be considered.
    - If an adult (over 18) is involved then police involvement will be required. Contact 101 or 999 if there is risk of immediate harm.
- Is the child able to understand the implications of taking/sharing sexual imagery?
- Is the school or other agencies aware of any vulnerability for the children(s) involved? E.g. special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved? E.g. family situation, children at risk of sexual exploitation?

Context

- Is there any contextual information to help inform decision making?
    - Is there indication of coercion, threats or blackmail?
    - What was the intent for taking/sharing the imagery? E.g. was it a "joke" or are the children involved in a "relationship"?
        - If so is the relationship age appropriate? For primary schools a referral to social care regarding under age sexual activity is likely to be required.
    - Is this behaviour age appropriate experimentation, natural curiosity or is it possible exploitation?
- How were the school made aware of the concern?
    - Did a child disclose about receiving, sending or sharing imagery themselves or was the concern raised by another pupil or

    member of the school community? If so then how will the school safeguard the pupil concerned given that this is likely to be distressing to discuss.

- Are there other children/pupils involved?
    - If so, who are they and are there any safeguarding concerns for them?
    - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?
- Is the imagery on a school device or a personal device? Is the device secured?
    - **NB: Schools and settings must NOT print/copy etc. imagery suspected to be indecent – the device should be secured until advice can be obtained**

The Imagery

- What does the school know about the imagery? (Be aware it is unlikely to be necessary for staff to view the imagery)
    - Is the imagery potentially indecent (illegal) or is it "inappropriate"?
    - Does it contain nudity or sexual acts?
- Does the child(ren) know who has accessed the imagery?
    - Was it sent to a known peer (e.g. boyfriend or girlfriend) or an unknown adult?
- How widely has the imagery been shared? E.g. just to one other child privately, shared online publically or sent to an unknown number of children/adults?

Action

- Does the child need immediate support and or protection?
    - What is the specific impact on the child?
    - What can the school put in place to support them?
- Is the imagery available online?
    - If so, have appropriate reports been made to service providers etc.?
- Are other schools/settings involved?

    - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in youth produced sexual imagery concerns before?
    - If so, what action was taken? **NB repeated issues will increase concerns for offending behaviour and vulnerability therefore an appropriate referral will be required.**
- Are the school child protection and safeguarding policies and practices being followed?
    - Is a member of the child protection team on hand and is their advice and support available?
- How will the school inform parents?
    - With older pupils it is likely that DSLs will work with the young person to support them to inform parents
- Can the school manage this issue internally or are other agencies required?
    - Issues concerning adults, coercion or blackmail, violent/extreme imagery, repeated concerns, vulnerable pupils or risk of significant harm will always need involvement with other agencies.

DSLs should follow the guidance available locally by East Sussex LSCB and the SLES Safeguarding Team and nationally via "'Sexting in schools: youth produced sexual imagery and how to handle it" which can be downloaded from the UKCCIS website: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

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/