Online Safety (e-Safety) Handbook (Incorporating the Acceptable Use Policy

February 2019

ARCHBISHOP SENTAMU ACADEMY

Church of England

"I have come that they may have life, and may have it in all its fullness" John 10:10.

Approved by Archbishop Sentamu Academy Principal on 13 February 2019

Next review date: February 2020

Archbishop Sentamu Academy

Christian Aims and Values

Values

Inspired by God: Father, Son and Holy Spirit we **Aspire** to be a community founded upon mutual trust where everyone is loved for who they are. We seek to **Serve** others by putting their needs before our own and believe that working together, with God's help, we can **Achieve** more than we could alone.

As a Church of England Academy, our core values are trust, love and community:

- **Trust** is essential to human life and lies at the heart of all successful relationships. With wisdom and understanding, we can learn to trust. We aim to do this by being reliable and not letting others down. In this way we, can help each other feel safe;
- Jesus has shown us love. We try to reflect that **love** to those around us by being sensitive to the needs of all members of our Academy community;
- We aim to be an inclusive **community**. Each person is needed, valued and important. When things go wrong we will forgive each other and make a fresh start. We will share what we have with those in need and try to treat others as we would like them to treat us.

Aims

As a Church of England Academy we aim to:

- Treat students, staff and visitors with respect;
- Incorporate and promote the values behind the academy motto; Aspire, Serve, Achieve in all we do;
- Instil a sense of self-worth and value in every student;
- Encourage student participation in the planning and the running of our Academy wherever possible;
- Encourage religious literacy as a way of interpreting the world around us;
- Encourage, challenge and support every person to achieve his or her potential.

Contents

Archbishop Sentamu Academy

1. Introduction

Online safety or e-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy is intended to address all rights, privileges and responsibilities associated with the use of computers and the internet at Archbishop Sentamu Academy.

The Academy's Online Safety (e-Safety) policy will operate in conjunction with other policies including those for Social Networking, Student Behaviour, Anti-Bullying, Curriculum, Data Protection and Child Protection.

2. Risks

Though the Academy seeks to encourage the use of online technologies with our young people, it is important that we are reminded of the risks posed from them. A significant number of safeguarding issues can be facilitated through digital technologies, and whilst the breadth of issues classified within online safety is considerable, we can classify them into three distinct areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes harm

3. Good Habits

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of online safety policy in both administration and curriculum, including secure Academy network design and use.

- Safe and secure broadband including the effective management of content filtering.

- National Education Network standards and specifications.

4. Academy e-Safety

The Academy will appoint an online safety group. This will be the Child Protection Coordinator, Designated Safeguarding Lead and the Online Safety Coordinator.

The online safety Policy will be reviewed at least annually.

5. Why is Internet use important?

The purpose of Internet use in Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our Academy has a duty to provide students with quality Internet access.

Students will use the Internet outside Academy and will need to learn how to evaluate Internet information and to take care of their own safety and security.

6. How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient (online teaching and learning resources, facilitating 24:7 'anywhere' access).
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DFE

7. How can Internet Use Enhance Learning?

- The Academy Internet access will be designed expressly for student use and includes filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

8. Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before being given their log-in details and using any Academy ICT resource.
- Students will not be given log-in details until they have agreed to comply with the online safety statement within their planners.
- Parents will be asked to sign and return a consent form within Academy planners for student access
- The Academy will maintain a current record of all staff and students who are granted Internet access.
- Parents, students and staff will be informed that Internet access will be monitored.

9. World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time and content must be reported to their Teacher or RM (as appropriate).
- Archbishop Sentamu Academy will ensure that the use of Internet derived materials by students and staff complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

9.1 *Social Networking* (please refer to the Social Networking Policy Appendix E for further guidance in this area)

- The Academy will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students should be advised not to place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted

communications. Students should be encouraged to invite known friends only and deny access to others.

- Staff should never make contact with any students via Facebook or other social networking sites. Any attempt to contact staff by students should be reported to the Designated Safeguarding Lead and Assistant Vice Principal in charge of ICT.

9.2 Filtering

- The Academy will work in partnership with its Internet Service Provider to ensure filtering systems are as effective as possible (to prevent downloading / viewing of 'unsuitable information / content').

- Internet usage and filtering is monitored using Smoothwall for all users of ICT within the academy. E-safety on all academy devices is monitored using Securus. ICT use may be monitored live using RM tutor and Apple remote desktop within the Academy. In addition e-safe is used to monitor network usage, including key strokes, websites accessed and searched for, and content on the network, such as images and documents. Any inappropriate network use is logged, monitored and actioned accordingly (see Appendix b and c)

9.3 Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

9.4 Assessing Risks

The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of Internet access.

The online safety group will audit at least annually ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

9.5 Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. This includes racist influences and extremist views from the far right which might affect our young people. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child

Protection Co-ordinator / Designated Safeguarding Lead). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils.

9.6 Access to inappropriate images and appropriate Internet usage

There are no circumstances that will justify adults possessing indecent images of children. Staff and students who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Staff and students should not use equipment belonging to the Academy to access adult pornography; neither should personal equipment containing these images or links to them be brought into the Academy. This will raise serious concerns about their suitability to continue to work and or study at the Academy.

Staff should be alert to and ensure that children and young people are not exposed to any inappropriate images or web links.

Where indecent images of children or other unsuitable material are found, the Child Protection Officer should be immediately informed (depending on material / circumstances the police and Local Authority Designated Officer (LADO) may also be informed). Staff should not attempt to investigate the matter or evaluate the material themselves, this is a matter for the Child Protection Officer to deal with and wherever possible staff should not view indecent images taken of young people as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Staff and students are prohibited from using the computer to perpetuate any form of fraud, or software, film or music piracy.

All members of our community are expected to use the Academy Internet in a responsible and appropriate way. It is not acceptable to access online betting websites (or websites relating to this), pornographic material, websites that promote race hate or criminal activities or websites that break copyright rules (e.g. illegal file sharing sites etc.) or any other website that might be deemed inappropriate.

If staff are at any time unsure of whether a website could be perceived as being inappropriate they are advised not to access it and seek advice from their department SLT link. If you accidently access inappropriate material please inform the Designated Safeguarding Lead and Assistant Vice Principal in charge of ICT immediately.

9.7 *Remote Access*

Remote access to the Academy network is possible via the internet or a Virtual Private Network (VPN). Remote access from external networks or across the internet must be made via secure methods only. Remote access is subject to the same conditions, requirements and responsibilities as onsite facilities.

10. Email

- Students may only use approved e-mail accounts on the Academy system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff should not disclose any personal details about themselves when communication via email to students.
- All communication with students should be through the Academy email system (i.e. @sentamuacademy.org) and not through staff members personal email accounts.
- Access to external personal e-mail accounts may be blocked within the Academy.

11. Managing Emerging Technologies / Mobile Telephones

- Students are not permitted mobile telephones within in the Academy.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed.
- www.keepkidssafe.co.uk is the chosen method of SMS contact with parents and students.

12. Published Content and the Academy Web Site

- The contact details on the Web site will be the Academy address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Vice Principal with responsibility for ICT will take overall editorial responsibility and ensure that content is accurate and appropriate.

13. Publishing Students' Images and Work

- Photography and Video: Working with children and young people may involve the taking or recording of images. Any such work should take place with due

regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is published for any purpose. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet.

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained annually before photographs of students are published on the Academy Web site.
- Work can only be published with the permission of the student and parents the Academy will keep a central list of those parents objecting.

14. Information System Security

- Academy ICT systems capacity and security will be reviewed regularly by RM.
- Virus protection software will be installed and updated regularly by RM.
- Security strategies will be reviewed by the e-Safety group.
- Laptops (supplied by the Academy) should be connected to the Academy network at least once per calendar month to allow for anti-virus scans / updates to occur and software updates to be installed.
- RM will regularly check user files, temporary Internet files and history files and report any concerns to the Vice Principal with responsibility for ICT.
- Uploading and downloading of non-approved application software is denied.
- All access to the Academy network requires entry of a recognised User ID and password. Students must log out after every network session. Staff must not leave their computers logged in when unattended.
- Staff and students must not disclose their password to anyone.

15. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and successor legislation. See separate Data Protection Policy.
- Staff and students must not publish confidential or defamatory and/or knowingly false material about the Academy, staff, students or anyone associated with the Academy on social networking sites, 'blogs' or any other online publishing format.

16. Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures

All other complaints will be dealt with via the Academy Complaints Procedure (for staff/parents) a copy of which is available on the Academy website or upon request. Staff complaints will be dealt with via the Grievance Procedure which is available from Human Resources.

17. Communication of Online Safety Expectations

17.1 *Students*

- Rules for Internet access will be posted in all ICT suites and included in Student planners.
- Students will be informed that Internet use will be monitored and recorded.
- Advice and online safety information available to students via Archbishop Sentamu Academy Website (under “Internet Safety” link)

17.2 *Staff*

- All staff will be given the Academy e-Safety handbook and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

17.3 *Parents*

- Parents’ attention will be drawn to the Academy Online Safety expectations in newsletters, via the Academy Facebook page and on the Academy Web site
- Advice and online safety information available to parents via Archbishop Sentamu Academy website (under “Internet Safety” link)
- Online Safety awareness sessions will be offered to parents/carers – these will run on selected parent information evenings
- Parents should be aware that the Academy will take any reasonable action to ensure the safety of its’ students: in cases where the Academy has reason to be concerned that any child may be subject to ill-treatment, neglect or any other form of abuse, the Academy has no alternative but to follow the Archbishop Sentamu Academy Child Protection Policy and inform Children’s Services of their concern.

17.4 *Visitors*

- Visitors / guests to Archbishop Sentamu Academy must abide by online safety procedures and policies as set out in this handbook in the same way as staff and students.
- Any visitor/guest who will have access to the Academy network will be required to sign the Staff Acceptable Use Policy.
- Visitors/Guests will be unable to access the Wi-Fi network using personal devices, unless permission is sought from the AVP in charge of ICT.

18. Breaches of Online Safety and Sanctions

18.1 *Staff*

Where it is believed that a staff member has failed to comply with the guidelines within this handbook they may be subject to the Academy's Disciplinary procedure. If they are found to have breached the ICT Acceptable Use agreement or Online Safety Handbook guidelines, they will face a penalty ranging from a verbal warning to dismissal. The actual penalty will depend on factors such as the seriousness of the breach and their disciplinary record.

18.2 *Students*

Where it is believe that a student has failed to comply with the guidelines within this handbook they may be subject to the Academy's Sanctions procedure. It they are found to have breached to policy they will face an appropriate sanction from a record in their planner to permanent exclusion. Temporary or permanent loss of network or internet access may also be considered. The actual penalty will depend on factors such as the seriousness of the breach and the student behaviour record.

19. Communicating with children and young people (including the use of technology)

Communication between children and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Staff should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Staff should ensure that all communications are transparent and open to scrutiny. Archbishop Sentamu Academy has mobile phones available to staff for occasions when it may be

necessary to phone pupils, for example, on an educational visit. Staff should not have the mobile phone numbers of pupils stored on their own phones.

Staff should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites for example Social networking sites such as Facebook and Twitter.

Internal e-mail systems should only be used to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management information and administration systems.

20. Online Sexual Harassment

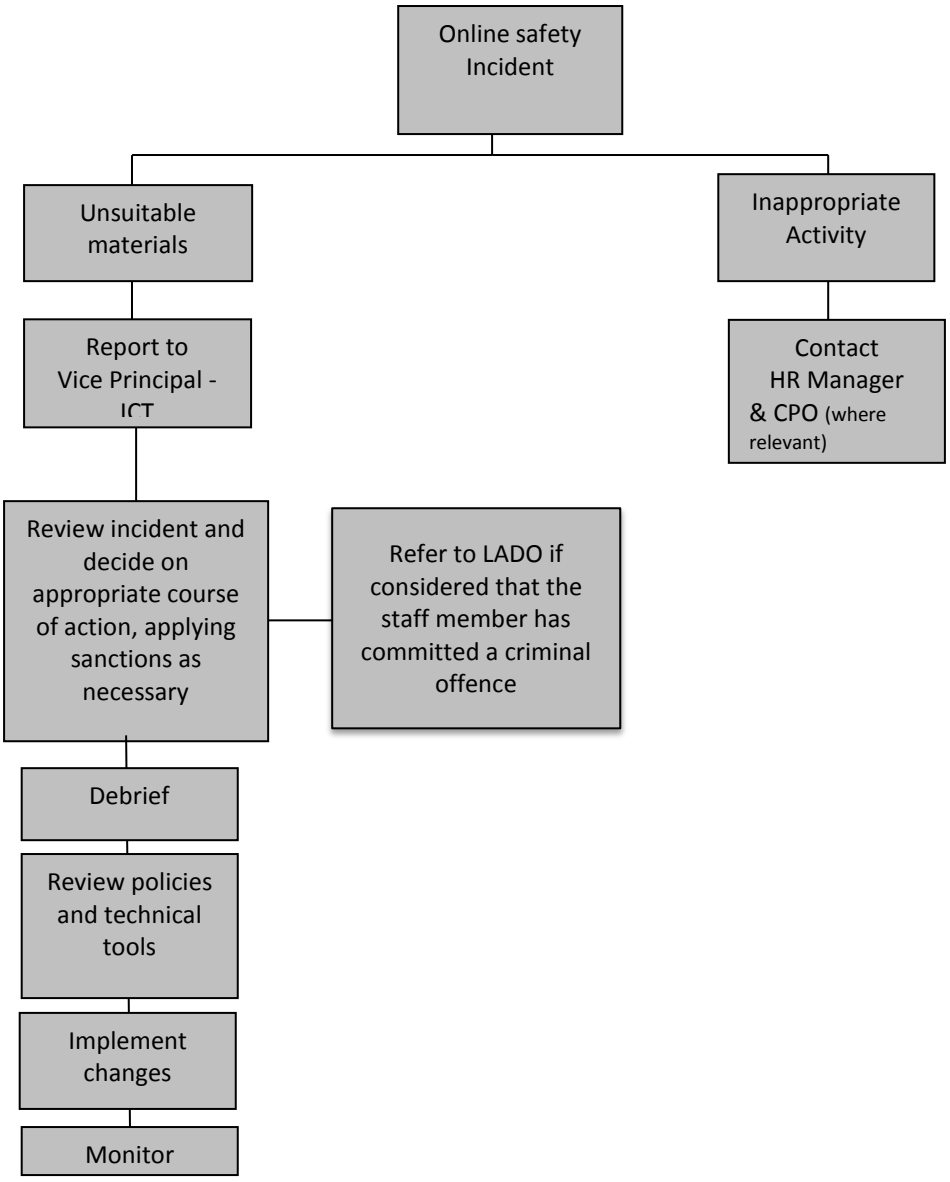
Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our Academy follows and adheres to the national guidance- UKCCIS: sexting in schools and colleges: responding to incidents and safeguarding young people, 2016

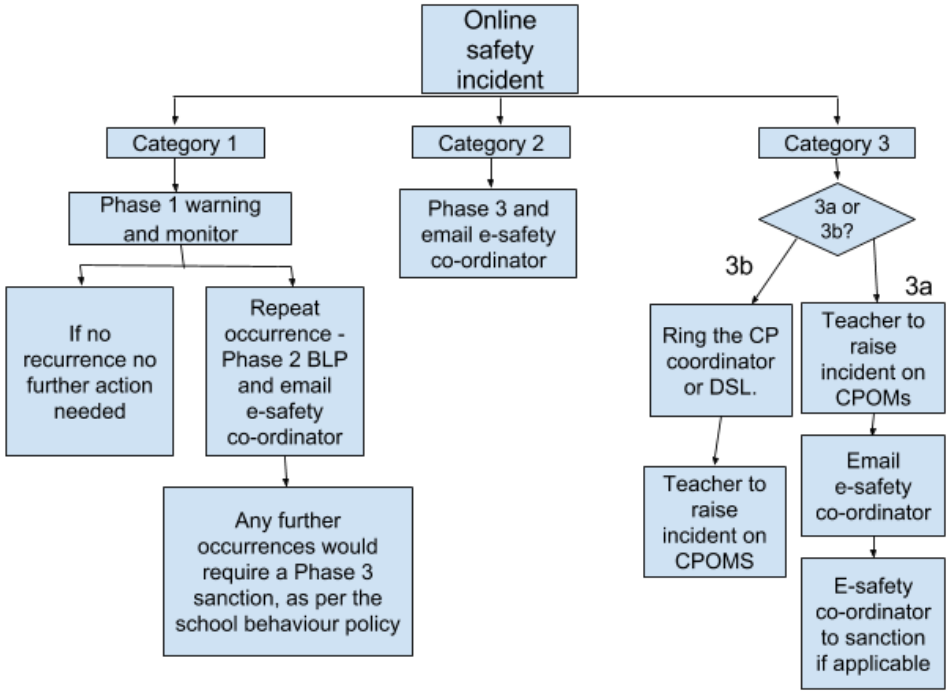
Appendix A - Referral Process for staff

Flowchart for responding to staff online safety incidents in Academy



Appendix B - Referral Process for Students

Flowchart for responding to online safety incidents with students in the Academy

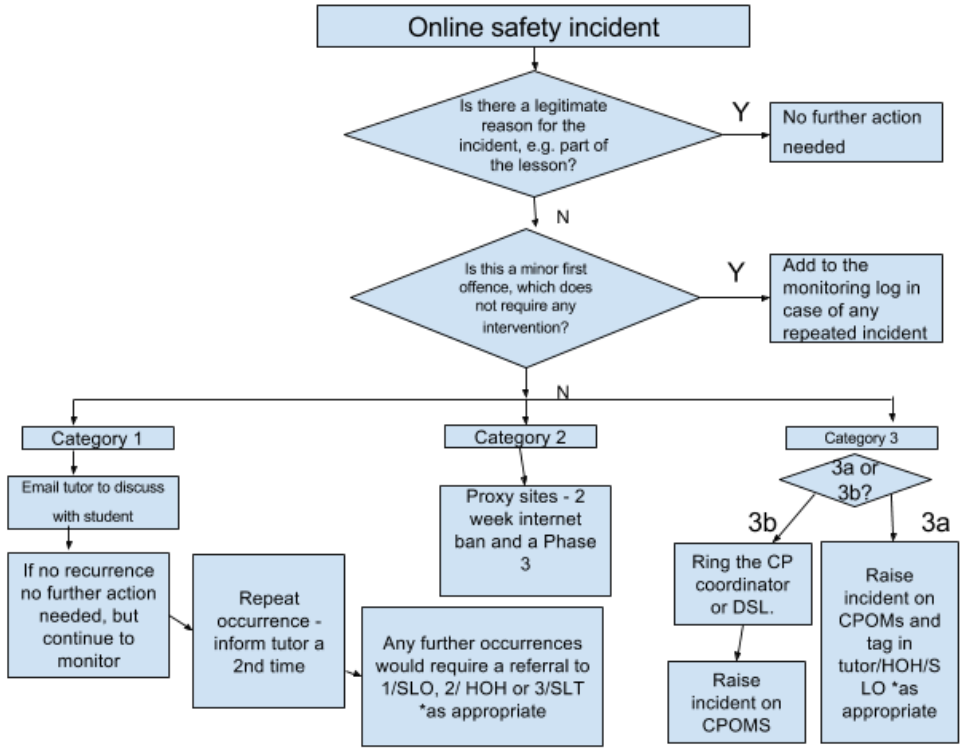


|

Key		
Category 1 incidents	Those incidents which are not deemed to be serious but are not correct use of the school network and could pose an online safety threat.	Example incidents: *typing something silly/inappropriate into Google translate or a search engine, online games, Youtube videos which are not appropriate to the lesson...*
Category 2 incidents	Those incidents which are a more serious breach of the school network rules	Example incidents: *searching for proxy sites in order to bypass the school network or where the student is using someone else's account.*
Category 3 incidents	3a - Those incidents which are of concern, either because of the nature of the search or the content 3b - As above, but which could also lead to the child being at risk of significant harm.	Example incidents which should be raised on CPOMS: *student searching for weapons, illegal substances or illegal content (such as pornography).* Example incidents *which could indicate the child is at risk of significant harm: arranging to meet up with a stranger, searching for things to do with self-harming or committing suicide, sexting.*

Appendix C - Referral Process for Monitoring using esafe (Students)

Flowchart for responding to online safety incidents with students in the Academy



Key		
Offences that would not require intervention	Those incidents which are a first offence and are deemed not serious.	Example incidents: *Student types a silly username into Kahoot (a site teachers use as starters and plenaries)*
Category 1 incidents	Those incidents which are not deemed to be serious but are not correct use of the school network and could pose an online safety threat.	Example incidents: *typing something silly/inappropriate into Google translate or a search engine, online games, searching for inappropriate/non-work focused images (first offences)*
Category 2 incidents	Those incidents which are a more serious breach of the school network rules	Example incidents: *searching for proxy sites in order to bypass the school network or where the student is using someone else's account.*
Category 3 incidents		

Appendix D - What to do if an issue is reported to you

If a child, young person or adult discloses information to you that they have been a victim of some form of abuse online, it is important to stay calm and listen to what they have to say. If dealing with such a situation, the following advice should be considered:

Do

- Be accessible and receptive
- Listen carefully
- Take it seriously
- Reassure the child that that they are right to tell
- Say what will happen next
- Consult immediately using CPOMs
- Make a careful record of what was said

Don't

- React strongly, e.g. by saying "how disgusting"
- Jump to conclusions, especially about the abuser
- Speculate or accuse anybody
- Tell the child you will keep their secret
- Ask any leading questions
- Make promises you cannot keep
- Stop a child who is speaking freely
- View or make a copy of any images which the child may have sent to the abuser

Useful phrases:

- *"What you are saying is very important to me and I will treat it as such"*
- *"I'm glad you were able to tell me/someone"*
- *"I will help you as best as I can"*
- *"This is so important I need to speak to someone who can do something about what is happening to you"*

*Guidance adapted from the NSPCC Keeping Children Safe Online course, 2016

Appendix E – Letter to Parents

Student Name: **Tutor group:**

Student's Agreement

- I have read and I understand the Academy Online Safety Rules
- I will use the computer, network, mobile phones, internet access and other new technologies in a responsible way at all times.
- I know that network and internet access maybe monitored and recorded.

Signed: **Date**

Parent's consent for Web Publication of Work and Photographs

I agree/disagree* that my son/daughter's work may be electronically published.
*delete as appropriate
I understand that the Academy will seek separate consent to publish images and videos that include my son/daughter.

Parent's consent for internet access

I have read and understood the Academy Online Safety rules and give permission for my son / daughter to access the Internet. I understand that the Academy will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the Academy cannot be held responsible for the content of materials accessed through the Internet. I agree that the Academy is not liable for any damages arising from use of the Internet facilities.
I am aware of the Academy Acceptable Use Policy and Online Safety policies and will support the schools approach to online safety.
!, with my child, will not upload, share or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community.

Signed: **Date:**

Please print name:

Please complete, sign and return to the Academy

Appendix F - Online Safety Rules for learners

These Online Safety Rules help to protect students and the Academy by describing acceptable and unacceptable computer use.

- The Academy owns the computer network and can set rules for its use.
- It may be a criminal offence to use a computer or network for a purpose not permitted by the Academy.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers. This includes text messages sent from mobile phones. Users should consider the feelings of others and not post hurtful or damaging images or text
- Anonymous messages and chain letters/emails are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The Academy ICT systems may not be used for private purposes, unless the Principal has given specific permission.
- I will not leave my computer unattended without first locking the computer or device, or logging off the network.
- I will not attempt to access any computer systems or data that I have not been given explicit permission to access and understand that doing so is likely to constitute a criminal offence under the Computer Misuse Act, and where personal data is accessed an offence under the Data Protection Act and successor legislation.

The Academy will exercise its right to monitor and keep a record of the use of the Academy's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the Academy's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Learner Online Safety (e-Safety) Rules.

Print Name: ……

Signed: ……

Date: ……

Appendix G - Staff Acceptable Use Policy

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the Academy's online safety handbook for further information and clarification.

- The information systems are Academy property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that Academy information systems may not be used for illegal or pornographic purposes.
- I understand that the Academy may monitor and record my information systems and Internet use to ensure policy compliance and for lawful purposes.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely.
- I will not allow access to my computer or mobile electronic device with automatic access to the academy network or email to anyone else including my family.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Assistant Vice Principal with responsibility for ICT or the Designated Child Protection Coordinator .
- I will report any incidents regarding the loss of personal data to the Data Protection Officer.
- I will ensure that any electronic communications with students, parents/carers and other professionals are compatible with my professional role and the expectations outlined in this document.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not undertake any deliberate ICT activity that wastes staff effort or resources.
- I will not use a colleague's credentials to access the networks or systems and will ensure that my credentials are not shared and are protected against misuse; and,
- I will protect all credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share any password other than for the purposes of placing a secured copy in a secure location at my employer's premises);and,
- I will not attempt to access any computer system or data that I have not been given explicit permission to access and understand that doing so is likely to

constitute a criminal offence under the Computer Misuse Act, and where personal data is accessed an offence under the Data Protection Act and successor legislation; and,

- I will not transmit information via any network that I know or suspect to be unsecure, and,
- I will not make false claims or denials relating to my use of the network (e.g. falsely denying that an e-mail had been sent or received); and,
- I will protect any information sent, received, stored or processed by me to the same level as I would paper copies of similar material; and,
- I will always check that the recipients of e-mail messages are correct to prevent personal or otherwise confidential information being disclosed in error or not reaching the intended recipient; and,
- I will seek to prevent inadvertent disclosure of personal or otherwise sensitive information by avoiding being overlooked when working, by taking care when printing information (e.g. by using printers in secure locations or collecting printouts immediately when they have printed etc) and by carefully checking the distribution list for any material to be transmitted; and,
- I will securely store or destroy any printed material; and,
- will not leave any computer unattended without first locking the computer or device, or logging-off the network; and,
- where the school and/or its IT provider(s) has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout or automatic screen locking), then I will not attempt to disable such protection; and,
- if I detect, suspect or witness any incident that may result in unauthorised or inappropriate access to data or the loss, damage or unintended destruction of data I will report the details to the Data Protection Officer at the earliest opportunity and,
- I will not attempt to bypass or subvert system security controls or to use any system for any purpose other than that intended; and,
- I will not remove equipment or information from school premises or any data from systems without appropriate prior authorisation; and,
- I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car to invite an opportunist theft); and,
- I will not knowingly introduce viruses, Trojan horses or other malware into the network or systems; and,
- I will not disable anti-virus protection provided at my computer; and,
- I will comply with the Data Protection Act 1998 and successor legislation and any other legal, statutory or contractual obligations that the school informs me are relevant; and,

- if I am about to leave the school, I will inform my manager prior to departure of any important information held in my account and manage my account, and any records which I have created or maintained, in accordance with the school's policies and procedures.

The Academy may exercise its right to monitor and record the use of the Academy's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the Academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Personal Commitment Statement

I understand and agree to comply with the security rules of my organisation. I accept that I have been granted the access rights to the school's information, IT network and systems. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access data or systems that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by these guidelines, this personal commitment statement and the school's data protection policy.

I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the school's disciplinary policies. I also understand that the school is required to report any potentially criminal acts to the police and/or the Information Commissioner's Office who may take separate action against me.

I have read and understood the school's Data Protection Policy and agree to work in accordance with it.

I have read, understood and agree with the Staff Acceptable Use Policy in relation to information systems.

Print Name: ……

Signed: ……

Date: ……

Please sign and return a copy of this page to, Human Resources

Appendix H - Wi-Fi Acceptable use policy

As a professional organisation with responsibility for children's safeguarding it is important that all users of the academy Wi-Fi are fully aware of the boundaries and requirements when using the Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the academy are reminded that ICT use should be consistent with the academy ethos, other appropriate policies and the Law.

Please be aware that Archbishop Sentamu Academy will not be liable for any damages or claims of any kind arising from the use of the wireless service. The Academy takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the Academy premises that are not the property of the Academy.

Archbishop Sentamu Academy allows access to the Wi-Fi for education use only.

1. The use of ICT devices falls under the academy's Acceptable Use Policy and behaviour policy (any other relevant policies (e.g. data security, safeguarding/child protection) which all students/staff/visitors and volunteers must agree to, and comply with.)

2. The academy reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. Academy owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the academies service is adequately secure (such as up-to- date anti-virus software, systems updates).

5. The wireless service is not secure, and the academy cannot guarantee the safety of traffic across it. Use of the Archbishop Sentamu Academy wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the academy harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. The academy accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the academy wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the academy from any such damage.

7. The academy accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the academy wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate

9. I will not attempt to bypass any of the security and filtering systems or download any unauthorised software or applications.

10. My use of the academy WiFi will be safe and responsible and will always be in accordance with the Acceptable Use Policy and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Claire Boyton) or the Vice Principal (Anthony Bennett) as soon as is possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online Safety (e-Safety) Coordinator or the Assistant Vice Principal responsible for ICT.

14. I understand that my use of the academy internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the academy suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the academy terminates or restricts usage. If the academy suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree with the WiFi Acceptable Use Policy.

Print Name: ……

Signed: ……

Date: ……

Please sign and return this page to Mandy Watson, Human Resources Manager

Appendix I -Use of Cloud Systems Permission Form

Archbishop Sentamu Academy uses Google Apps for Education for pupils and staff. This consent form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil and hosted by Google as part of the academy's online presence in Google Apps for Education:

- Mail - an individual email account for school use managed by the academy
- Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments
- Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
- Sites - an individual and collaborative website creation tool

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The academy believes that use of the tools significantly adds to your child's educational experience.

Students over 13 will be able to give their own consent to use Google Apps for Education.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Use of Cloud Storage Systems – Parental Consent	
Child's Name …….	Class……
Parents Name ……..	
Parents Signature…….	Date……

Appendix J – Social Networking Policy

Archbishop Sentamu Academy

1. INTRODUCTION TO THE POLICY

The academy is aware and acknowledges that increasing numbers of adults and children are using social networking sites. This policy includes a wide range of sites, such as Instagram, LinkedIn and YouTube. The two with the widest use currently are Facebook and Twitter.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance is to protect staff and advise academy leadership on how to deal with potential inappropriate use of social networking sites.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

2. PURPOSE

The purpose of this policy is to ensure:

- That the academy is not exposed to legal risks
- That the reputation of the academy is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the academy.

Facebook is targeted at older teenagers and adults. They have a no under 13 registration policy and recommend parental guidance for 13 to 16 year olds. The following are extracts from Facebook privacy policy:
"If *you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as*

quickly as possible. If you believe that we might have any information from a child under age 13, please contact us"… "We *strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices.*

Materials to help parents talk to their children about safe internet use can be found on the Facebook help page.

Twitter no longer appears to have a policy of debarring younger pupils.

Instagram and Youtube require everyone to be at least 13 before they create an account.

The guidance provided within this document is to advise and protect staff from accusations of improper relationships with pupils.

3. SCOPE

This policy covers the use of social networking applications by all academy stakeholders, including, employees, volunteers, trainee teachers, supply staff, Governors and pupils. These groups are referred to collectively as 'academy representatives' for brevity.
The requirements of this policy apply to all uses of social networking applications which are used for any academy related purpose and regardless of whether the Academy representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:

- Blogs, for example Blogger
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media sharing services, for example YouTube
- 'Micro-blogging' applications, for example Twitter

All academy representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the Academy's Equality and Diversity Policy.

4. USE OF SOCIAL NETWORKING SITES IN WORK TIME

Use of social networking applications during work time for personal use only is not permitted, unless permission has been directly given by the Principal. This includes on the use of own equipment e.g. mobile phone.

5. SOCIAL NETWORKING AS PART OF ACADEMY SERVICE

All proposals for using social networking applications as part of a academy service (whether they are hosted by the academy or by a third party) must be approved by the Principal first

Use of social networking applications which are not related to any academy services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Principal. However, academy representatives must still operate in line with the requirements set out within the policy.

Academy representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all academy representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on academy network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Archbishop Sentamu Academy expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

5.1 Terms of Use - Social Networking applications

5.2

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the academy into disrepute.

- Must not be used in an abusive or hateful manner

- Must not be used for actions that would put academy representatives in breach of academy codes of conduct or policies relating to staff.

- Must not breach the academy's misconduct, equal opportunities or bullying and harassement polices

- Must not be used to discuss or advise any matters relating to academy matters, staff, pupils or parents

- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with

- No staff member should have a pupil or former pupil as a 'friend' to share information with if they were on the academy roll less than 12 months ago, regardless of age

- Employees should not identify themselves as a representative of the academy

- References should not be made to any staff member, pupil, parent or academy activity / event unless prior permission has been obtained and agreed with the Principal

- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

5.2 Guidance/protection for staff on using social networking

- No member of staff should interact with any pupil in the academy on social networking sites

- No member of staff should interact with any ex-pupil in the academy on social networking sites who is under the age of 18. In addition the ex-student must also have not been on roll at the academy for at least one calendar year.

- This means that no member of the academy staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.

- Where family and friends have pupils in academy and there are legitimate family links, please inform the Principal in writing. However, it would not be appropriate to network during the working day on academy equipment

- It is illegal for an adult to network, giving their age and status as a child

- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection person in academy

- References to the academy should not be made on social networking sites unless you have expressed permission to do so from the Principal

5.3 Guidance/protection for Pupils on using social networking

- No pupil under 13 should be accessing social networking sites. This is the guidance from a range of providers. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is: http://www.facebook.com/help/contact.php?show_form=underage

- No pupil may access social networking sites during the academy working day

- No Pupil should use social networking sites to harass other student's including harassment of a sexual natural

- All mobile phones are not allowed in the academy

- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Principal. Parents will be informed if this happens

- No academy computers are to be used to access social networking sites at any time of day.

- Any attempts to breach firewalls will result in a ban from using academy ICT equipment other than with close supervision

- Please report any improper contact or online bullying to you tutor / class teacher in confidence as soon as it happens.

- We have a zero tolerance to online bullying

6. Child protection guidance

If the Principal receives a disclosure that an adult employed by the academy is using a social networking site in an inappropriate manner as detailed in section 5.2, he/she should:

- Record the disclosure in line with the academy child protection policy. The academy must refer the matter to Humberside Police. *LADO – follow the procedures for dealing with allegations outlined in the CP policy, it depends on the activity, advice should be initially sought from the LADO in the first instance*

- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes

- If disclosure comes from a member of staff, try to maintain confidentiality.

- The LA will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
  If disclosure is from a child, follow the normal process in the child protection policy until the police investigation has been carried out.

7. Online Bullying

By adopting the recommended no use of social networking sites on academy premises, Archbishop Sentamu Academy protects themselves from accusations of complicity in any online bullying through the provision of access.

Parents should be clearly aware of the academy's policy of access to social; networking sites.

Where a disclosure of bullying is made, we now have the duty to investigate and protect, even where the bullying originates outside the academy.

This can be a complex area, and these examples might help:

- A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not an academy responsibility, though the academy might contact the new academy to broker a resolution.
  A child is receiving taunts from peers. It is all at weekends using Twitter and Facebook. The pupils are in the academy: The academy has a duty of care to investigate and work with the families, as they attend the academy.

  A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y7: This is the tricky one. The academy has a duty of care to investigate and work with the families, as they attend the academy. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. If this is not successful we would review how else we could protect the pupil. Once disclosure is made, investigation will have to involve the families. This should be dealt with under the academy's anti-bullying policy.

If parent / careers refuse to engage and bullying continues, it can be referred to the police as harassment.

This guidance can also apply to text and mobile phone online bullying.

8. Sexting

What is sexting?

Sexting is considered by many professionals to be the sending or posting of sexually suggestive images, including nude or semi-nude photographs, via phones or over the internet. The advice written here is intended to be used when dealing with the sharing of sexual imagery by young people. This is illegal and is a complex issue which must be dealt with appropriately.

Other language used by young people: Young people may also refer to this practice using the terms 'trading nudes', 'dirties', 'underwear shots' or 'pic for pic'.

What does the law say?

The law is clear – making, processing and/or distributing any imagery of someone under 18, which is 'indecent' is illegal. Despite this, the police will not usually wish to criminalise young people for such behaviour. For this reason, as of January 2016 in England and Wales, if a young person is found creating or sharing images, the police (if informed), will still record the incident as a crime, with the young person being listed as a 'suspect', but they can choose not to take any formal action if this is not deemed to be in the public interest. It would be unlikely that such recorded crimes would appear on future checks, such as on a DBS certificate, unless the young person had been involved in other similar activities which may indicate that they are a risk.

How should I handle any incidents that come to my attention?

When handling an incident to do with 'youth produced sexual imagery', the incident must always be recorded on CPOMs as soon as is reasonably possible. You should also notify Julie Allinson or Claire Boyton as a matter of urgency, either in person or via mobile phone.

If the incident involved a device (such as a mobile phone), ask the young person to turn it off, and then confiscate the device. This should then be handed in to the Designated Safeguarding Lead or Child Protection Co-ordinator as soon as possible.

IMPORTANT: Adults should NOT view youth produced sexual imagery wherever possible.

If you have unavoidably come across an image (for example if it was on a school networked device),
it is important to:

- Never copy, print or share the imagery – this is illegal

- Refer the matter immediately to the Assistant Vice Principal in charge of online safety or to the Child Protection Co-ordinator or Designated Safeguarding Lead.

If you require any further information or assistance with how to respond to incidents, please email Vicky Moore on moore.v2@sentamuacademy.org .

Useful links

There is a vast array of information available to support teachers in keeping children safe online. The following links are a useful starting point for anyone seeking to find out more information:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org

www.educateagainsthate.com

https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF