2019

E-Safety Policy

SMART MULTI-ACADEMY TRUST

Document Control		
Author(s):	Chris Haves	External V1.0
Updated by:		16/01/2019
Trustee Committee Approval		
Board Approval Date	16/01/2019	
Chair of Trustees' Signature:		
Next Review Date:	January 2022	
Review Cycle:	3 Years	

Version Log

Document Title:		E-Safety Policy	
Author(s)		C.Haves	
Version number:		1.0	
Date of review:		January 2022	
Document History			
Version	**Date**	**Author**	**Note of revisions**
1.0	16/01/2019	C.Haves	New Policy ratified by the Board of Trustees on 10.01.2019

Table of Contents

1.0 Introduction *5*
2.0 Teaching and learning *6*
2.1 Background **6**
2.2 Why is Internet use important? **6**
2.3 Education – Pupils **7**
2.4 Education – Parents / Carers **7**
2.5 Education – The Wider Community **8**
2.6 Education & Training – Staff / Volunteers **8**
2.7 Training – Governors **8**
3.0 Use of mobile devices *9*
3.1 Mobile Phones **9**
3.2 Laptops **10**
4.0. Use of digital media (cameras and recording devices) *11*
4.1 Consent and Purpose **11**
4.2 Taking Photographs / Video **11**
4.3 Parents Taking Photographs / Videos **11**
4.4 Storage of Photographs / Video **12**
4.5 Publication of Photographs / Videos **12**
4.6 CCTV, Video Conferencing, VOIP and Webcams **12**
5.0. Communication technologies *13*
5.1 How is email managed? **13**
5.2 Trust/School website **13**
5.3 Publishing Pupil Images? **13**
5.4 How can emerging technologies be managed? **14**
5.5 Social Networks **14**
6.0. Infrastructure and technology *16*
6.1 Pupils' access **16**
6.2 Adult access **16**
6.3 Passwords **16**
6.4 Software/hardware **16**
6.5 Managing the network and technical support **16**
6.6 Filtering and virus protection **17**
6.7 Assessing Risks **17**
7.0. Dealing with incidents *18*
7.1 Handling online safety complaints **18**
7.2 Cyberbullying **18**

8.0 Disseminating the policy *20*
8.1 Sharing with pupils **20**
8.2 Sharing with staff **20**
8.3 Engaging parents **20**
Annex 1: Legal Requirements *21*
Annex 2: Contacts *24*

1.0 Introduction

Online safety refers to not only Internet technologies but also electronic communications. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. This encompasses:

- Safeguarding children and young people in the digital world.
- Learning to understand and use technology in a positive way.
- An Approach that is less about restriction and more about education and understanding risks so we can feel confident online.
- Supporting children and young people to develop safer online behaviours both in and out of school.

The Trust Online Safety Policy reflects the importance it places on the safe use of information systems and electronic communications. This policy, supported by the Trust's Technology Acceptable Use Policy, is to protect the interests and safety of the whole school community. It is also linked to the following mandatory policies around:

- Child Protection
- Health and Safety
- Home-School Arrangements
- Behaviour and Anti Bullying
- PSHE
- Corporate ICT

Internet technologies and electronic communications provide children and young people with 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.

This E-Safety policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure.

Smart Multi-Academy Trust (the Trust) is committed to ensuring that all children across all Trust schools are able to learn and develop using technology in a safe environment.

Where reference is made to the Trust, this is trust wide across all schools sites.

2.0 Teaching and learning

2.1 Background

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to worldwide educational resources.
- Inclusion in the National Education Network (www.nen.gov.uk) which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and access to learning wherever and whenever convenient.

Our aim is to produce learners who are confident and effective users of Computing. We strive to achieve this by:

- Helping all pupils to use computing with purpose and enjoyment.
- Helping all pupils to develop the necessary skills to exploit computing.
- Helping all pupils to become autonomous users of computing.
- Helping all pupils to evaluate the benefits of computing and its impact on society.
- Meeting the requirements of the National Curriculum and helping all pupils to achieve the highest possible standards of achievement.
- Using computing to develop partnerships beyond the school.
- Celebrating success in the use of computing.

2.2 Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. Computing skills and knowledge are vital to access life-long learning and employment; indeed computing is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils must be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhance the Trust's management information and business administration systems.

2.3 Education – Pupils

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The Online Safety Curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils must be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff temporarily remove those sites from the filtered list for the period of study. Any request to do so, must be auditable, with clear reasons for the need and in coordination with ICT Support.

2.4 Education – Parents / Carers

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, websites, VLE, blogs, Facebook
- Parents' sessions
- High profile events / campaigns

2.5 Education – The Wider Community

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

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

2.6 Education & Training – Staff / Volunteers

It is essential that all Trust staff receive Online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online safety training is made available to staff. This will be regularly updated and reinforced. An audit of the Online safety training needs of all staff will be carried out regularly.
- All new staff receive Online safety training as part of their induction programme, ensuring that they fully understand the Trust Online safety policy and Acceptable Use Agreements.
- The Online safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events.
- This Online safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Online safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

2.7 Training – Governors

Governors will have the opportunity to take part in online safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in Trust/school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

3.0 Use of mobile devices

3.1 Mobile Phones

Mobile phones are now a feature of modern society and it is likely most older pupils have one. The technology of mobile phones has developed such that they now have the facility to access the internet, record sound, take photographs and video images. The Trust recognises the advantages mobile phones have as a ubiquitous learning tool. However, this new technology is open to abuse leading to the invasion of privacy.

Increasing sophistication of mobile phone technology presents a number of issues for schools:

- They are valuable items that may be stolen.
- The integration of cameras into phones leading to potential child protection and data protection issues.
- The potential to use the phone e.g. for texting whilst on silent mode.
- Inappropriate messages being sent via SMS, including Cyberbullying and sexual harassment.
- Interruption to lessons and disrupting the learning of others.

Staff

In accordance with the Smart Technology Acceptable Use Policy:

- All staff mobile phones must be either switched off or on silent and locked in a secure area during the school day.
- No member of staff must use a personal mobile phone in the presence of pupils.
- Mobile phones may be used during break times but only in areas of the school designated as acceptable by the Headteacher (e.g. staffroom).
- Staff must keep personal phone numbers private and not use their own mobile phones to contact pupils or parents.
- It is expected that at least one member of staff will carry a mobile phone when off site with pupils (for example for school excursions) and in line with the school's Business Continuity Plan.
- If school/Trust information is stored on a mobile phone (including access to email or remote storage), the phone must be encrypted.
- If a mobile phone containing school/Trust information is lost or stolen, the school Headteacher and Trust Data Protection Officer must be informed, as this may need to be reported as a data breach.

Pupils

- Phones must always be switched off (not on silent mode) and handed in to a teacher or the school office before the start of the school day, to be collected at the end of the day.
- All pupil phones must be password protected.
- If a pupil needs to contact his/her parents/guardians they will arrange to use the landline in the school office.
- If parents need to contact their children urgently they must always phone the school office
- The Trust/school accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile phones.
- It is the responsibility of parents and pupils to ensure mobile phones are adequately insured.

- If a pupil breaches these rules, the phone will be confiscated and taken to the main office. It will be returned to the parent at the end of the school day.

Visitors

- All visitors will refrain from using their mobile phone in school in the presence of pupils. Mobile phone use is restricted to just those areas designated as acceptable by the Headteacher.

3.2 Laptops

- Staff provided with a laptop purchased by the Trust can only use it for private purposes at the discretion of the Headteacher/CEO. Such laptops remain the property of the Trust and are open to scrutiny by senior management, contracted technicians and the computing subject leader. Any use must be in line with the Staff Technology acceptable use policy.
- If a personal laptop is required to hold Trust information, this must be done in accordance with the Technology Acceptable Use Policy.
- All laptops across the Trust must be encrypted.
- Laptops belonging to the Trust must have updated antivirus software installed and be password protected.
- Staff must not connect personal laptops to the Trust/school network, unless it is through visitor Wi-Fi using and an appropriate login.
- The security of Trust/school laptops is of prime importance due to their portable nature and them being susceptible to theft. Safety of laptops is the responsibility of the member of staff to which they are allocated
- If a laptop (either personal or Trust owned) containing school/Trust information is lost or stolen, the school Headteacher/CEO and Trust Data Protection Officer must be informed immediately.

4.0. Use of digital media (cameras and recording devices)

4.1 Consent and Purpose

- Parents will give consent at the beginning of each school year or on entry to school for photographs/videos of their children to be taken or used. They may also be asked to give consent for certain activities children will be taking part in during the school year.
- Staff, volunteers and governors will give written consent at the beginning of each school year or on entry to school for photographs of themselves to be taken or used (where this is not covered by a legal basis for processing outlined in the Trusts Privacy Notice).
- It will be made clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of third parties).
- All media storage is done so in accordance with the Trusts' Information Management Policy.
- Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journals and portfolios, press / other external media.
- The names of children and adults who have requested that their photographs will not be taken will be held on each schools Management Information System.

4.2 Taking Photographs / Video

- All members of staff are authorised to take photographs/videos
- All photographs/videos must be taken using Trust/school owned equipment. The use of personal equipment to store images is not allowed
- When taking photographs/ video:
    - The rights of an individual to refuse to be photographed will be respected
    - The photograph will not show children who are distressed, injured or in a context that could be embarrassing or misinterpreted
    - Ensure that certain children are not continually favoured when taking images
    - Ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted. This would include for example, considering the angle of shots for children engaged in PE activities
    - Photographs of children or adults must not be taken in toilets or when changing in the changing rooms

4.3 Parental Photography/Videos

Under the Data Protection Act (2018), parents are entitled to take photographs of ***their own*** children on the provision that the images are for ***their own*** use. However, it is difficult to ensure that other pupils are not included in media so this is difficult to police.

Where permission has been granted for parents to take photographs:

- Parents are informed that they must only take photographs of their own children and that they need permission to include any other children/adults.
- Parents may be asked to wait until the end of an event to take photographs/videos so as not to disrupt the event.

- Parents are reminded in writing, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects.

4.4 Storage of Photographs / Video

- The storage of photographs and video is done in accordance with Trusts' Information Management Policy.
- Photographs are securely stored on the Trust/school network.
- Storage of photographs on portable storage (such as USB memory sticks) is not allowed.
- Storage of images on personal equipment e.g. tablets, laptops or USB storage devices is not allowed.
- School staff have access to photographs/videos stored on Trust/school equipment.
- Trust/school staff are responsible for deleting photographs/video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed.
- Must a parent withdraw permission for photographs/videos; a nominated member of staff will ensure that all images have been securely deleted.
- All images sent via email must be sent securely using file encryption and a secure password.

4.5 Publication of Photographs / Videos

When publishing images,

- Children's images must only be displayed, where relevant parental consent has been gained and is limited to the school website, Trust website and school social media accounts.
- No photographs must be put onto personal social media accounts.
- Full names and personal details will not be used on any digital media, particularly in association with photographs/ videos.
- Where images/videos are required to be put onto a separate website (e.g. for a newspaper article) separate consent will be sought (in line with the Trusts Privacy Notice).

The Media, third Parties and Copyright

- Third Parties must be supervised at all times whilst in the school and must be wearing the correct lanyard linked to their DBS check.
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc, the terms and conditions of the website must be read beforehand and agreed by the Headteacher/DPO. The website upload portal must be verified as secure.

4.6 CCTV, Video Conferencing, VOIP and Webcams

- Parents are informed if CCTV, video conferencing or webcams are being used / in use in the school. This is in line with the Trusts CCTV policy.
- The Trust has a specific image and video policy, which all staff must read and adhere to
- Video conferencing (or similar) sessions must be logged including the date, time and the name of the external organisation/ person(s) taking part

- The purpose for video conferencing or webcams will be made clear to those liable to be included in footage taken by these resources.
- Notifications are in place to inform setting users that CCTV is being used
- Any CCTV cameras located throughout the school both indoors and outdoors do not overlook sensitive areas, e.g. changing rooms or toilets.
- All CCTV screens must have restricted access (not communal area) and only be visible to those with the approved access.

5.0. Communication technologies

5.1 How is email managed?

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Email sent to external organisations must be written carefully in the same way as a letter written.
- The forwarding of chain messages is not permitted.
- Staff must not use personal email accounts during school hours or for professional purposes.
- Any email containing personal information must be encrypted using appropriate software.
- If personal information is being transferred, alternative should be considered (such as shared cloud storage).

5.2 School website

- The contact details on the website must be the school address, email and telephone number.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website must comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The school website must contain all statutory information outlined by the DFE.

  https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

5.3 Publishing Pupil Images

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Consent from parents or carers must be obtained before images of pupils are electronically published (parental consent form).
- Pupils' work can only be published in accordance with relevant consent from the Pupil Accomplishment and Activities Parental consent form.

5.4 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice if classroom use is to be developed.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The Computing Co-ordinator will carry out each risk assessment – this must be done in conjunction with ICT Support.

5.5 Social Networks

- Any use of personal social media sites must comply with the Trust Technology Acceptable Use Policy, which if breached could lead to disciplinary action.
- If a social network site is used personally, staff must not share details with pupils and privacy settings must be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Staff must not give personal contact details to pupils or parents / carers.
- Staff must not befriend pupils or parents on social networking sites (except in certain circumstances e.g. friends/family and where approved by the Headteacher/CEO).
- Staff must not use school equipment to communicate with personal contacts (e.g. FaceTime on an iPad).
- The content posted online must not:
    - Bring the Trust/school into disrepute
    - Lead to parental complaints
    - Be deemed as derogatory towards the Trust/school and / or its employees
    - Be deemed as derogatory towards pupils and / or parents and carers
    - Bring into question staff appropriateness to work with children and young people

Following a report of inappropriate use of social networking sites, the nominated person will take the following action.

- Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed.

- If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. The material posted may breach the service provider's terms and conditions of use and can then be removed.

- In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider. Some service providers will not accept complaints lodged by a third party.

In cases of mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.

- Before the nominated person contacts a service provider, he or she will check the location of the material – for example by taking a screen capture of the material that includes the URL or web address. If the nominated person is requesting that the service provider takes down material that is not illegal, he or she will be clear how it contravenes the site's terms and conditions.

Where the perpetrator is a member of the Trust community (including parents/carers) the Trust/school will:

- Deal with harassment and bullying under the relevant Trust procedure
- take care to make an informed evaluation of the severity of the incident
- deliver appropriate and consistent sanctions; and
- Provide full support to the staff member(s) affected.

The Trust Board/Local Governing Board recognises its legal duty to protect staff from unlawful harassment as well as mental and physical injury at work.

In cases of potentially criminal content, the nominated person will consider whether the police must be involved, following appropriate liaison with staff, and parents where necessary.

6.0. Infrastructure and technology

6.1 Pupils' access

- Pupils are supervised by an adult when accessing school equipment and online materials.
- Pupils have restricted access to the school's network.

6.2 Adult access

- Access to certain areas of the school's network are restricted to identified members of staff according to their areas of responsibility.

6.3 Passwords

- All users of the Trust/school network have a secure username and password.
- Staff are reminded of the importance of keeping passwords secure.

6.4 Software/hardware

- The Trust has legal ownership of all software (including apps on tablet devices).
- Where applicable, appropriate licenses for all software will sit with the School Business Manager or ICT Support.
- Equipment and software is audited on an annual basis. Each school and ICT Support hold an Asset Register of all ICT equipment.
- ICT Support will support the installation of software on school systems (once it has been approved).

6.5 Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access is restricted.
- Wireless devices are accessible only through a secure password.
- The IT technician (through ICT Support) is responsible for managing the security of the school network and keeping the school systems up to date in terms of security.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password and permissions are assigned according to their role.
- Staff and pupils are required/reminded to lock or log out of a school system when a computer/digital device is left unattended. By way of a safeguard, IT policy automatically locks a machine has been inactive for a set period.
- The IT technician (through ICT Support) is responsible for assessing and installing new software.
- Any suspicion or evidence of a breach of security must be reported to the Headteacher and Data Protection Officer.
- The IT technical support provider is aware of the school's requirements / standards regarding online safety.
- Computing subject leader and the Headteacher are responsible for liaising with the technical support staff.

6.6 Filtering and virus protection

- Website and email filtering is managed through ICT Support.
- Any site requiring blocking or unblocking must be approved by the Headteacher and submitted to ICT support for approval.
- Any suspected or actual computer virus infection must be reported to the Headteacher and ICT support immediately.

6.7 Assessing Risks

- The Trust/school will take all reasonable precautions to prevent access to inappropriate material with corporate filtering systems. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never appear on a computer connected to the school network. The Trust or ICT Support does not accept liability for any material accessed, or any consequences resulting from Internet use.
- The final decision when assessing risks will rest with the CEO.

7.0. Dealing with incidents

7.1 Handling online safety complaints

- Complaints of computing/Internet misuse must be recorded and will be dealt with by the Headteacher who will decide if sanctions are to be imposed.
- Any complaint about staff misuse must be referred to the Headteacher who will decide if sanctions are to be imposed.
- Complaints of a child protection nature must be dealt with in accordance with Trust child protection procedures.
- The Headteacher will arrange contact/discussions with the Local Authority and the police to establish clear procedures for handling potentially illegal issues.
- Any complaint about illegal misuse must be referred to the Headteacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by the Local Authority.
- All staff, pupils and parents will be informed of the complaints procedure.
- All staff, pupils and parents will be informed of the consequences of misusing the Internet and computing equipment.
- Any suspected data breaches, complaints or issue relating to data protection must be referred to the Trust DPO.

7.2 Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the Trust's Anti-Bullying Policy.
- There will be clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyberbullying must be reported to the Headteacher at the earliest possible opportunity.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers must keep a record of any incident as evidence.

There will be clear procedures in place to investigate incidents or allegations of cyberbullying:

- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases will be dealt with most effectively under the relevant disciplinary procedure.
- Monitoring and confiscation must be proportionate to the incident. Except in exceptional circumstances (for example, where disclosure would prejudice the conduct of a criminal investigation) parents, employees and learners will be made aware, and their consent sought, in advance of any monitoring (for example, of e-mail or internet use) or the circumstances under which confiscation might take place.
- Where a potential criminal offence has been identified, and reported to the police, the Trust/school will ensure that any internal investigation does not interfere with police inquiries.
- Where pupils are found to have made unfounded, malicious claims against staff members, relevant disciplinary processes will be applied with rigour, as is the case in relation to physical assaults.

- Staff must report all incidents to the Headteacher. They will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period.
- Parent/Carers may be informed.
- The police will be contacted if a criminal offence is suspected.

8.0 Disseminating the policy

8.1 Sharing with pupils

- Online safety rules and posters will be displayed in all rooms where computers are used and highlighted/ discussed during computing sessions.
- Pupils will be made aware that the network and Internet use will be monitored.
- An online safety-training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
- An online safety module will be included in the computing scheme of work and PHSE curriculum.

8.2 Sharing with staff

- Staff will be consulted when creating and reviewing the Online Safety Policy.
- Staff training in safe and responsible Internet use, both professionally and personally, will be provided, including use of social networking sites such as Facebook.
- Every member of staff, whether permanent, temporary or supply, will be informed that Network and Internet traffic will be monitored and can be traced, ensuring individual accountability.

8.3 Engaging parents

- Parents'/carers' attention will be drawn to the Trust Online Safety Policy in newsletters, the school brochure and on the school website.
- A parents' workshop will be held annually to inform parents/carers about online safety issues and responsible use.
- Parents will be requested to sign an online safety/Internet agreement as part of the Home School Agreement.
- Information and guidance on online safety will be made available to parents/carers in a variety of formats.

Annex 1: Legal Requirements

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

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 that is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

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.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools must already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
More information about the 2003 Act can be found at www.teachernet.gov.uk

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 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.

Data Protection Act 2018 / General Data Protection Regulation (GDPR)

Any organisation that handles personal information to notify the Information Commissioner's Office of the type of processing it administers. It 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.

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.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) 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 can include racist, xenophobic and homophobic comments, messages etc.

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 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.

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.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another and which he 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.
This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) 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.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person's 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 can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools that relate to Cyberbullying/Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

Keeping Children Safe in Education 2018

This document sets out the legal duties schools must follow to safeguard and promote the welfare of children and young people under the age of 18 in schools and colleges. It contains numerous references to technology including in relation to radicalisation, cyber bullying, and abuse and neglect that tie into this policy and others (such as the Technology Acceptable use Policy)

Annex 2: Contacts

Where there is a reference to ICT Support, this is currently managed by either Newcastle City Council ICT Services

education.it@newcastle.gov.uk

Or Kenton ICT Support for Kenton Bar Primary

spicemail@kenton.newcastle.sch.uk

Data Protection Officer

DPO@smartacademies.net

Smart Central Support

Admin@smartacademies.net

Report a data security breach:

Link to the online data Breach form here or a hard copy of the form is available from school business managers or the DPO.