THEDWASTRE
Education Trust

Policy Name: ONLINE SAFETY POLICY

Original: May 2017 (Reviewed: October 2018)

Author: Head Teachers Leadership Group

Date ratified by the Trust Board: 25 October 2018

Date for review: October 2019

Publish on Trust website: Yes

Publish on Academy websites: Yes

Signed:

Chair of Directors

ONLINE SAFETY POLICY

(Acceptable use Agreements for the internet and other technologies)

Introduction

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of each academy to ensure that children and young people are protected from potential harm both within and beyond the academy environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies. Our academies reserve the right to take action and report inappropriate behaviour to the police.

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'online-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

Each academy will:

- emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school
- provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences
- ensure adults are clear about procedures for misuse of any technologies both within and beyond the school
- develop links with parents/carers and the wider community, ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies

"The internet and the use of social media in particular has become a major factor in the radicalisation of young people." (KCSIE, 2015)

As academies, we are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of our functions to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. The Prevent duty complements other key documents, guidance and advice including: Keeping children safe in education; Working together to safeguard children; Statutory Framework for the Early Years Foundation Stage - setting the standards for learning, development and care from birth to five. Our key aim is to protect children from the risk of radicalisation and ensure that we have the appropriate support mechanisms in place in order to protect children from this risk.

Roles and Responsibilities

Governors/Headteachers

It is the overall responsibility of the Headteacher with the Governors of each academy to ensure that there is an overview of online-safety as part of the wider remit of safeguarding across the academy, with further responsibilities as follows:

The Headteacher has designated an Online-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online-safety is addressed in order to establish a safe learning environment. All staff, students and parents are aware who takes this role within the academy.

- Time and resources should be provided for the Online-Safety Lead and staff to be trained and to update policies, where appropriate.
- The Headteacher is responsible for promoting online-safety across the curriculum and has an awareness of how this is being developed, linked with the School Development Priorities for the Academy/Trust.
- The Headteacher should inform the Curriculum Committee about the progress of or any updates to the online-safety curriculum (via PSHE or computing) and ensure Governors know how this relates to safeguarding. At Full Governing Body meetings, all Governors are to be made aware of online-safety developments from the Curriculum Committee chair or through the minutes of meetings.
- Governors MUST ensure online-safety is an integral part of safeguarding education and know how it is being addressed within the school. It is the responsibility of the Governing Body (or the designated Safeguarding Governor) to ensure that all safeguarding guidance and practices are embedded, including online safety.
- The governor responsible for online-safety must ensure that the academy has an Online-Safety and Acceptable Use Policy, and an Acceptable Use Agreement with appropriate strategies which define the roles and responsibilities for the management, implementation and safety of ICT. The responsible governor must be confident that the following safety measures are in place:

    - firewalls
    - anti-virus and anti-spyware software
    - filters
    - use of an accredited ISP (Internet Service Provider)
    - an awareness of wireless technology issues
    - a clear policy on using personal devices
    - This information may be sought from the school's IT technical support team

- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

Local Online-Safety Lead

It is the role of the designated Online-Safety Lead (this person should be a senior member of the academy staff and not a network manager) to:

- Appreciate the importance of online-safety within the academy and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the academy.
- Ensure that the Online-Safety and Acceptable Usage Policies are reviewed annually or when necessary, with up-to-date information, and that training is available for all staff to teach online-safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC and laptops or ensure the technician is informed to carry out this work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Safeguarding and ICT/Computing Leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct online-safety information can be taught or adhered to.
- Keep a log of incidents, which is separate from the general incidents log, for analysis to help inform future development and safeguarding, where risks can be identified - refer to the Managing Allegations Procedure from the SSCB to ensure the correct procedures are used with incidents of misuse.
- Work alongside the ICT/Computing Lead or network manager to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff alert the network manager if they suspect there is a virus on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received (www.Suffolkscb.org.uk/procedures/lscb-policies-guidance-and-protocols/SearchForm?Search=managing+allegations+procedure&action_results=Search)
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

Staff and/or Adults

It is the responsibility of all adults within the school to:

- Ensure that they know who is the Senior Designated Person (and the alternate) for Safeguarding within the academy, so that any misuse or incidents which involve a child can be reported.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Person and LADO.
- In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying, Prevent Strategy, Safeguarding Policy and other relevant policies so that, in the event of misuse or an allegation, the correct

procedures can be followed immediately. In the event that a procedure is unknown, staff will refer to the Headteacher/Senior Designated Person immediately, who should then follow the Managing Allegations Procedure, where appropriate.

- Check that filtering levels are appropriate for the children and young people and are set at the correct level before using equipment. Report any concerns to the Online-Safety Lead.
- Alert the Online-Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with online-safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Agreement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and do not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in. Ensure that a user logs off when they leave the station or the device unattended.
- Ensure that school bursars and other staff follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the Online-Safety Lead.
- Use anti-virus software and check for viruses on their work laptop, memory stick or CD when transferring information from the Internet, especially when not connected to the school's network.
- Ensure that all personal school storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the academy's accident/incident reporting procedure in the same way as for other non-physical assaults.

Children and Young People

Children and young people should be:

- Involved in the review of Acceptable Use Agreement through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Agreement whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Taught to use the Internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

All staff have a password to access a filtered Internet service which should not be disclosed to anyone. Staff must not leave a computer or other device unattended whilst they are logged in. Temporary staff will be given a guest password. Only staff and adults identified as having a need will be given a password to access the Internet.

All staff should receive a copy of the Online-Safety and Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file, with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the Internet, or photographic equipment such as mobile phones or digital cameras, in an abusive or illegal manner, a report must be made to the Headteacher immediately. The Headteacher will follow the Managing Allegations Procedure and the Safeguarding Policy to deal with any misconduct; all authorities will be contacted as appropriate.

Any device belonging to the academy will be closed down and isolated and the police will be informed.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

By Children or Young People

The Acceptable Use Agreement is outlined in the appendices. This details how children and young people are expected to use the Internet and other technologies within school, including the downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet. This will enable them to take responsibility for their own actions. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The academy should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

Downloading of materials, for example, music files and photographs, needs to be appropriate and ‘fit for purpose’, based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using them in or beyond school.

Each pupil has a unique password to access a filtered Internet service and know that this should not be disclosed to anyone. Children are taught not to leave a computer or other device unattended whilst they are logged in.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the Internet whilst at school, and/or to fail to follow the Acceptable Use Agreement, the following consequences will occur:

- suspension of the child or young person's Internet use for a particular lesson or activity
- further misuse will result in not being allowed to access the Internet for a set period of time

In both cases, parents will be informed by letter and the pupil will be carefully observed once the suspension is lifted.

In the event that a child or young person accidentally accesses inappropriate materials, the child should report this to an adult immediately and take appropriate action to hide the screen or minimise the window so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the school.

The Trust reserves the right to confiscate and search any electronic device which has been brought into an academy, where it has been reported that the device has been used to bully, humiliate or deliberately upset another child or adult, invade privacy or to post indecent or racist images or words. (Section 89 Education and Inspections Act 2006). Such a search will be made by two members of staff; an academy may request that a search is completed by police officers.

The Curriculum and Tools for Learning

Internet Use

Academies will teach children and young people how to use the Internet safely and responsibly. They should also be taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave Year 6:

- internet literacy
- making good judgements about websites, social media and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any online technologies
- knowledge of copyright and plagiarism issues
- file sharing and downloading illegal content

- uploading information – know what is safe to upload (being careful with personal information)
- where to go for advice and how to report abuse

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt a 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

Personal safety – ensuring information uploaded to web sites, social media, apps and e-mailed to other people does not include any personal information such as:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address (unless sending an e-mail)
- name of school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the school football team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded.

Pupils with Additional Learning Needs

The academy will provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration will be given to the planning and delivery of online-safety awareness sessions and Internet access.

Any relevant information regarding individual pupils will be passed on to the receiving school when a child transfers.

School Website and Twitter Account(s)

The uploading of images to the school website and Twitter account(s) should be subject to the same acceptable agreement as uploading to any personal online space. Permission is to be sought from the parent/carer prior to the uploading of any images. Images may be uploaded with faces blurred so that pupils cannot be identified. Staff must not identify pupils by name alongside a photo on the school website or school social media account.

External Websites

In the event that a member of staff finds themselves or another adult victimised on an external website, such as 'Rate My Teacher', the member of staff should report the incident to the Headteacher, using the academy's reporting procedures. Staff are advised to inform their union.

E-mail Use

The school should have email addresses for children and young people to use, as a class and/or as individuals as part of their entitlement to being able to understand different ways of communicating and to share and present information in different forms.

Staff, children and young people should use their school issued email addresses for any communication between school, other educational establishments and parents/carers home email address only. A breach of this will be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent and received from home.

Teachers are expected to monitor their class use of emails on a regular basis.

Mobile Phones and Other Emerging Technologies

Pupil's mobile phones

Our academies allow Year 5 and Year 6 pupils to bring mobile phones on to the academy premises. These are handed to the school office during school hours and returned to the child at the end of the school day. If a child is found to use their mobile phone inappropriately, they will be barred from bringing it onto the school site for a fixed period and their parents will be informed. Inappropriate use includes:

- inappropriate or bullying text messages
- images or videos taken of adults or peers without permission being sought
- any breach of the Acceptable Use Agreement
- **mobile phones may not be turned on while on the school premises**

Staff and personal mobile devices

Staff are allowed to bring personal mobile phones or devices for their own use. These must not be used in the classroom or any learning based area unless after school once pupils have gone home. Staff must not use personal numbers to contact children and young people under any circumstances.

Staff must ensure that there is no inappropriate or illegal content stored on any personal device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.

Staff must not use personal devices for filming or photographing children.

Staff should be aware that games consoles such as the Sony PlayStation, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include

filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.

The Trust is not responsible for any theft, loss or damage of any personal mobile device.

Parents working in school on a voluntary capacity are subject to the same rules as staff – including use of mobile devices on trips.

The school reserves the right to allow photographs or films of performances and events but requests that parents do not upload images to social media when they contain images of children other than their own.

School Issued Mobile Devices

The management of the use of these devices should be the same as stated above, but with the following addition:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop or mobile phone, this equipment only (ie no personal devices) must be used to conduct school business outside of the school environment.

Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school there is access to camcorders, class digital cameras and tablets. Staff mobile phones, or personal photographic equipment, must not be used to take images or videos of pupils.

The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by the parent/carer and/or the members of staff who are featured in the photographs.

Photographs/images used to identify children and young people in a forum should be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child.

Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children/young people should only be used after permission has been given by a parent/carer.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (See Acceptable Use Agreement).

Managing Social Networking and Other Web 2.0 Technologies

The Trust prohibits pupils using any social networking sites, e.g. Facebook and Twitter, in any of its academies or on academy owned devices.

Social Networking Advice for Staff

Social networking outside of work hours, on non-school issue equipment, is the personal choice of all school staff. School equipment, including teacher laptops and the school mobile phone, should not be used with personal social profiles. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation.

All teaching and non-teaching staff working in education needs to ensure, both for the school's safety and their own, that activity on social networking sites: does not bring the school into disrepute, does not bring the teacher into disrepute, does not expose the school to legal liability, reflects 'safer internet' practices, minimises risks associated with the personal use of social media by professionals and reflects the school's standard of behaviour and staff code of conduct.

The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of authorised Academy systems (e.g. academy email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).

Filtering and Other Online Protection

- The broadband connectivity has a filter system which will be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child.
- Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.
- A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Monitoring

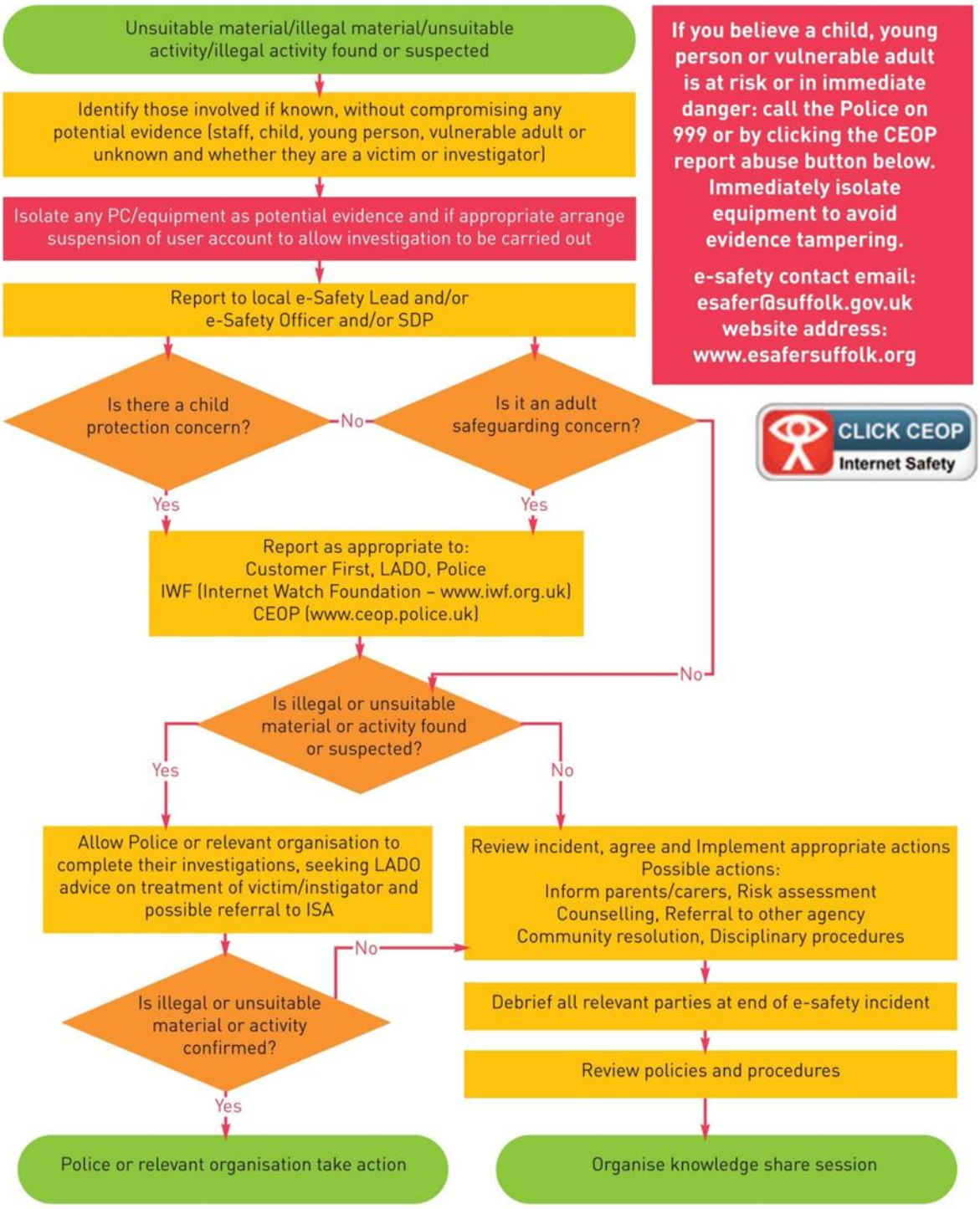
- The Online-Safety Lead is responsible for monitoring the use of online technologies by children and young people and staff, on a regular basis.
- Teachers should monitor the use of the Internet during lessons and also monitor the use of e-mails sent by pupils on a regular basis.
- Links to Other Policies - Behaviour and Anti-Bullying Policies.
- Academies will follow their Behaviour/Anti-bullying Policies when applying sanctions following behaviour or bullying incidents via any online communication, such as mobile phones, e-mail or blogs.

Health and Safety

Refer to the Health and Safety Policy for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

Appendix 1:

e-Safety Incident Flowchart



Appendix 2:

Acceptable Use Agreement for Staff, Governors and Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults working within the Thedwastre Education Trust must be aware of their safeguarding responsibilities when using any online technologies, such as the Internet, e-mail or social networking sites. Staff are required to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Online-Safety and Acceptable Use Policy so that I can effectively deal with any problems that may arise through misuse by pupils, staff or myself.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person or Online-Safety Lead in accordance with procedures listed in the Online-Safety and Acceptable Usage Policy.
- I know who the Senior Designated Person (and alternate) is in my academy.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones (if provided) and only to a child's school e-mail address upon agreed use within the school.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or Online-Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- Misuse of school equipment and any act that brings the school/academy into disrepute may result in disciplinary action.
- I have been given a copy of the e-Safety and Acceptable Usage Policy to refer to about all e-Safety issues and procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…….Date…….

Name (printed)…….

Academy ……..……

Appendix 3:

Acceptable Use Policy for Young People

My Online-Safety Agreement – Years 3, 4, 5 & 6

This is my agreement for using the Internet safely and responsibly:

- I will use the Internet to help me learn.
- I will learn how to use the Internet safely and responsibly.
- I will only send email messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to put online photographs or video clips without permission and I will never use my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the Internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my Internet in a safe and responsible way.

Signed..... Dated.....

Name.....(Printed)

Academy…….

Appendix 4:

Acceptable Use Policy for Young People

My Online-Safety Agreement – Years R, 1 & 2

This is my agreement for using the Internet safely and responsibly:

- I will only go on the internet if an adult supervises me.
- I will use the Internet to help me learn.
- I will not talk or type messages to people I don't know.
- I will always be polite and friendly to people on the Internet.
- I will never tell anyone on the Internet anything about me, except my first name, unless my teacher says I can.
- I will tell a teacher if I see or hear something I don't like.

Signed..... Dated.....

Name.....(Printed)

Academy……...