E-SAFETY POLICY

Policy Version			
Date	**Document Version**	**Document Revision History**	**Document Author/Reviser**
14.4.16	1.0	Revised document from AH (provided by Place Group on AH conversion	A White
16.3.17	1.1	Revised document following enhancement to E-Safety across the Trust.	Z.Pilkington
25.05.17	1.2	Update in light of LGB & Trust review/approval	Jayne Carmichael

This policy will be reviewed every 12 months or in light of a change to local and Government legislation.

The Dunham Trust believes it makes a significant contribution in transforming children's life chances. Our aim and commitment is to transform schools into sustainable learning academy communities.

"We aim to ensure that, for everyone involved, excellence and equity become and remain a reality"

"They come this way only once so we should litter their pathways with quality experiences"

We believe that we are able to help our academies and their young people to aspire to and achieve success. To do this, we are committed to ensuring that every child and young person has a pathway to succeed that:

- gives the best possible start in life
- equips them with creativity, spirit and confidence
- enables individuals to appreciate life and equip for further learning
- supports the child in becoming a responsible citizen
- ensures continued success in his/her future and contributes to the local community

Our aims for 'Improvement' are designed to ensure all academies are consistently benchmarked against key improvement priorities. This framework will ensure effective progress across the Trust, whilst at the same time, leaving space for autonomy at the school level. It will:

- focus efforts on what really matters, i.e. our vision, principles and commitment to the children, young people, families and communities that we serve.
- provide a flexible approach to improvement that meets the needs of each Academy. This will involve a commitment to immediate improvement in each individual context, professional development and a collaborative approach that engages with improvement projects designed to build capacity, an approach that is responsive, reflective and sustainable.
- focus on outcomes, understanding that these are not negotiable. We are committed to a no-excuses culture. In achieving these outcomes, all will focus on individual responsibility and collective accountability for success

The Trust has a responsibility to ensure the success of each academy by allowing every pupil to maximise his/her potential. As an academy sponsor there will be an expectation for joint working across individual academies. The Trust is committed to high quality academy improvement activity, networking and development and research. Equally, the promotion of sport, outdoor education and the creative arts will be important in the development of pupil self-esteem and building learning skills.

Contents

Introduction

The Dunham Trust recognises that it has an important duty to provide children with safe access to high-quality digital information and access to the internet. Schools within The Dunham Trust will teach children to be confident and highly competent digital users, who are also alert to the risks and dangers which the internet and digital world presents. While each school will use approved filtering systems and a range of preventative measures to ensure pupils' safety, The Dunham Trust recognises that away from the school, children are potentially less safe: by teaching active e-safety awareness, The Dunham Trust believes it will best prepare children for life in a dynamic digital world.

Our vision is that all schools within The Dunham Trust become e-confident schools. All members of our school communities: staff, pupils, parents and governors will confidently and safely make full use of the rich range of digital resources which empower each person to improved effectiveness and increased access to knowledge, skills and accelerated achievement.

E-Safety Audit – Primary

This self-audit should be completed by the member of the COMPUTING coordinator. Many staff will contribute to the audit, or support the completion, including: Designated Child Protection Coordinator, SENCO, Network Manager and Head of School

Audit

Has e-safety training been provided for both pupils and staff? Y/N

Is there a clear procedure for a response to an incident of concern? Y/N

Have e-safety materials from CEOP and Becta been obtained? Y/N

Do all staff sign a Code of Conduct for COMPUTING on appointment? Y/N (see staff use policy)

Are all pupils aware of the School's e-Safety Rules? Y/N (see Computing policy)

Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? Y/N

Is personal data collected, stored and used according to the principles of the Data Protection Act? Y/N

Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. KCN, Regional Broadband Consortium, NEN Network)? Y/N

Has the school-level filtering been designed to reflect educational objectives and approved by SLT? Y/N

Related Legislation

We believe this policy relates to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 1998
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2011
- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Children Act 2004
- Education Act 2003

The following documentation is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Headteachers, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

Purpose

The Dunham Trust takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones
- Internet communications: e-mail and IM
- Webcams and videoconferencing
- Wireless games consoles.

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 should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

Receiving inappropriate content;

- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data.

It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. A summary of a school's safety responsibilities is outlined below.

Writing and Reviewing the E-safety Policy

Our e-Safety Policy has been written by the school, building on the LGFL e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors. The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies. All staff must read and sign the Acceptable Use Policy. Pupils should sign and return the e-Safety Rules consent form as part of the home school agreement. The e-Safety Policy will be made available to all staff, governors, parents and visitors through the website.

Teaching and Learning

The school will include e-Safety in the curriculum and this will be referred to in planning. Teachers should ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

Why the Internet and Digital Communications Are Important

Developing effective practice in Internet use for teaching and learning is essential. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. The Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Pupils 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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Internet Use Will Enhance Learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience. The school will audit their filtering systems regularly to ensure that inappropriate websites are blocked.

Pupils Will Be Taught How to Evaluate Internet Content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content

Managing Internet Access

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content. Searches and web addresses are monitored and the ICT technician will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found. Where staff, children or visitors find unblocked extremist content they must report it to a senior member of staff.

Monitoring children when they are online
Children in KS2 have an individual log-in so that individual activity online can be monitored.
EYFS and KS1 have a class log-in and teachers supervise children when they are using the internet.
When using I-pads usage is monitored through class groupings. I-pads are numbered and children in each class are assigned a number that they use when accessing I-pads. This allows our technical support staff to monitor what children are viewing on websites and other applications and the time that they are being used.

Information system security

- School COMPUTING systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Network manager

E-mail

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. The school should consider how e-mail from pupils to external bodies is presented and controlled. The forwarding of chain letters is not permitted

How Will E-mail Be Managed?

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students, staff, or within local and international school projects.

However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once e-mail is available it is difficult to control its content.

Procedures

In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses, such as Hotmail, should be avoided by all working in schools and staff should be required to use appropriate LA systems for professional purposes.

Individual pupil e-mails such as janet.brown@schoolname.trafford.sch.uk which allow pupils to send and receive messages to and from the wider world, need to be carefully allocated to appropriate situations and to support the learning in individual lessons.

Pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's e-safety and anti-bullying education programme.

Pupils need to understand good "netiquette", style of writing, (this links to English) and appropriate e-mail behaviour appropriate to their age.
[Please note: to achieve expected standards or above, pupils must have experienced sending and receiving e-mails.]

This school:

Does not publish personal e-mail addresses of pupils or staff on the school website. If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police. Accounts are managed effectively, with up to date account details of users. Messages relating to or in support of illegal activities may be reported to the authorities. Spam, phishing and virus attachment can make e-mail dangerous. Use filtering software to stop unsuitable mail.

Pupils:

Pupils are introduced to, and use e-mail as part of the COMPUTING scheme of work. Pupils are taught about the safety and "netiquette" of using e-mail i.e.

- Not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer
- That an e-mail is a form of publishing where the message should be clear, short and concise
- That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc
- To "Stop and Think Before They Click" and not open attachments unless sure the source is safe
- The sending of attachments should be limited
- Embedding adverts is not allowed
- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
- Not to respond to malicious or threatening messages
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
- That forwarding chain e-mail letters is not permitted

Pupils in KS2 sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with:

- Staff use LA e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- That e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school "house-style"
- The sending of attachments should be limited
- The sending of chain letters is not permitted
- Embedding adverts is not allowed
- Staff can only use the school domain e-mail accounts on the school system.

Published Content and The School Website

In accordance with the School's Information Published on Website Policy, the contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing Pupil's Images and Work

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs unless permission is granted by a parent/carer.

Written permission forms from parents or carers will be obtained before photographs of pupils are published on the school website and twitter.

Work can only be published with the permission of the pupil and parents/carers.

Pupil image file names will not refer to the pupil by name.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. This is part of the home school agreement.

Social Networking and Personal Publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils at safety meetings and through materials on the school website.

Cookies

Cookies are small text files, used by your Web browser to store visitor session data on your computer by Websites that you visit. They are commonly used on the Internet in order to make Websites work more efficiently and to enhance end user experience. (Please see cookie policy)

Managing Filtering

If staff or pupils come across unsuitable on-line materials, the site must be reported to the COMPUTING Coordinator. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Staff will be issued with a school ipad/digital camera or school phone where contact with pupils is required. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not be used during lessons or formal school time. All mobile phones carried by children will be handed into the school office at registration and collected at the end of the day. Only pupils who walk to school or home independently and have permission from the Head Teacher will be able to bring a phone to school The sending of abusive or inappropriate text messages is forbidden.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Access

All staff must read and sign the Staff Acceptable Use Policy before using any school COMPUTING resource.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. In addition children will have discussed with their teacher and parent an acceptable use contract.

At Key Stage 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. In addition, children must use an individual login and have signed the KS2 acceptable use contract.

Any person not directly employed by the school will be asked to sign an “acceptable use of school COMPUTING resources” before being allowed to access the internet from the school site.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.
The school cannot accept liability for any material accessed, or any consequences of Internet access. he school should audit COMPUTING use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling E-safety Complaints

Complaints of Internet misuse will be dealt with by a senior member of staff, unless it is the Head of School, where complaints will be sent to the Chair of Governors. Any complaint about staff misuse must be referred to the Head of School.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure. Pupils and parents will be informed of consequences for pupils misusing the Internet. All children will be taught to use the internet safely and the role of CEOP to monitor and report abuse Parents and pupils will need to work in partnership with staff to resolve issues.

Communications Policy

Introducing the E-safety Policy to Pupils

E-Safety rules and points will be planned for and taught within all COMPUTING units.
Pupils will be informed that network and Internet use will be monitored and appropriately followed up. They sign an internet usage contract and use logins that allow for the monitoring of online activity. E-Safety training will be embedded within the COMPUTING scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and The E-Safety Policy

All staff will be given the School e-Safety Policy and its importance explained.
Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
Staff that manage filtering systems or monitor COMPUTING use will be supervised by senior management and work to clear procedures for reporting issues.
Staff will use a child friendly safe search engine when accessing the web with pupils.

Enlisting Parents' and Carers' Support

Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website and at open evenings. The school will maintain a list of e-safety resources for parents/carers. The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school

Appendix 1: Summary of staff and student device use

Communication Technology	Staff				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones in school	*							*
Use of personal mobile phones in lessons		*						*
Use of personal mobile phones in social time	*							*
Taking images on personal mobile phones or other devices		*						*
Use of digital hand-held devices such as tablets e.g. iPads	*				*			
Use of personal non-school emails in school or on school network	*							*
Use of school email system for personal emails	*							*
Use of chat rooms and facilities		*				*		
Use of instant messaging		*						*
Use of social networking sites		*						*
Use of blogs		*				*		

Appendix 2: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Webquest UK
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Ask Jeeves for Kids Yahooligans CBBC Search
Exchanging information with other pupils and asking questions of experts via e-mail and blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation. E.g. Super club plus.	E-mail detectives. Kids safe mail.
Publishing pupils' work on school or other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on moderated sites and sites approved by E-safety co-ordinator.	Super Club Plus National Education Network Gallery.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought.	Learning Grids.

	File names should not refer to the pupils by name. Staff must ensure that published images do not breach copyright law.	
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and moderated should ever be used. Pupils should never give out personal information.	Espresso.
Audio and video conferencing to gather information and share pupils' work.	Pupils must be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational suppliers.	JANET Videoconferencing Advisory Service (JVCS)

Appendix 3i: Useful Resources for Teachers

BBC Stay Safe
http://www.bbc.co.uk/cbbc/help/web/staysafe

BECTA
http://www.becta.org.uk/

Chat Danger

http://www.chatdanger.com/

Child Exploitation and Online Protection Centre

http://www.ceop.gov.uk/

ChildNet

http://www.childnet-int.org/

ThinkUKnow Cyber Café

http://www.thinkuknow.co.uk/8%5F10/cybercafe/

Digizen

http://www.digizen.org/

Kent E-safety site

http://www.kenttrustweb.org.uk/kcn/e-safety_home.cfm

Kidsmart

http://www.kidsmart.org.uk/

ThinkUKnow

http://www.thinkuknow.co.uk/

NSPCC
https://www.nspcc.org.uk/

Appendix 3ii: Useful resource for parents

Family Online Safety Institute

http://www.fosi.org/cms/

Internet Watch Foundation

http://www.iwf.org.uk/

Internet Safety Zone

http://www.internetsafetyzone.co.uk/

Parent Centre

http://www.direct.gov.uk/en/Parents/index.htm

ThinkUKnow Parent site

http://www.thinkuknow.co.uk/parents/

NSPCC
https://www.nspcc.org.uk/

02 provided free mobile phone setting guidance for parents, regardless of the network being used

http://www.o2.co.uk/help/nspcc/child-protection

Parental Control
http://www.esrb.org/about/settingcontrols.aspx

PEGI ratings
http://www.pegi.info/en/index/

Internet matters – A support website for parents
http://www.internetmatters.org

Digital Parenting
http://vodafonedigitalparenting.co.uk/

CEOP (Child Exploitation Online Protection) CEOP is a national crime agency command
https://ceop.police.uk/safety-centre/

Appendix 4: Sexting Policy
(also known as Oversharing, please refer also to child protection policy.)

Children using the internet are at risk from sexting so it is important that staff are aware of the following policy.

Definition of 'sexting'

Sexting is when a young person takes an indecent image of their self and sends this to their friends or boy/girlfriends via mobile phones.
There are a number of definitions of sexting but for the purposes of this advice sexting is simply defined as images or videos generated:

- by children under the age of 18, or
- of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know. The problem is that once taken and sent, the sender has lost control of these images and these images could end up anywhere. They could be seen by your child's future employers, their friends or even by child sex offenders. By having in their possession, or distributing, indecent images of a person under 18 on to someone else – young people are not even aware that they could be breaking the law as these are offences under the Sexual Offences Act 2003. (CEOP, 2015)

There are many different types of sexting and it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. It is important to apply a consistent approach when dealing with an incident to help protect yourself, the school and the pupil. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All staff should be familiar with this policy.

Steps to take in the case of an incident :

STEP 1: Disclosure by a Pupil

Sexting disclosures should follow the normal safeguarding practices and protocols. A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to social services.
The following questions will help decide upon the best course of action:

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?

- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed? For example, is the Designated Safeguarding Lead (DSL) for child protection on hand and is their advice and support available?
- How widely has the image been shared and is the device in the pupil's possession?
- Is it a school device or a personal device?
- Does the pupil need immediate support and or protection?
- Are there other pupils and or young people involved?
- Do they know where the image has ended up?

This situation will need to be handled very sensitively. Whatever the nature of the incident, ensure school safeguarding and child protection policies and practices are adhered to.

STEP 2: Searching a Device – What Are The Rules?

In a school-based context, it is possible that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device. It is important to establish the location of the image but be aware that this may be distressing for the young person involved, so be conscious of the support they may need.

The revised Education Act 2011 brought to bear significant new powers and freedoms for teachers and schools. Essentially, the Act gives schools and/or teachers the power to seize and search an electronic device if they think there is good reason for doing so. The interpretation of this Act has not yet been tested consequently pupils are not allowed to have personal electronic items with them during the school day. (Children who have to bring a device and have permission must place this in the school safe at the start of the day and collect it at the end of the day.)

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device the following conditions should apply:

- The action is in accordance with the school's child protection and safeguarding policies
- The search is conducted by the Head or a person authorised by them
- A member of the safeguarding team is present
- The search is conducted by a member of the same sex

If any illegal images of a child are found, the person responsible for child protection should consider whether to inform the police. Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police. If an "experimental" incident is not referred to the police the reasons for this should be recorded in writing. Always put the child first. Do not search the device if this will cause additional stress to the pupil/person whose image has been distributed.

Never

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem.
- Print out any material for evidence
- Move any material from one storage device to another

Always

- Inform the school's Designated Safeguarding Lead for child protection (DSL)
- Record the incident on the safeguarding form
- Act in accordance with school safeguarding and child protection policies and procedures
- Inform relevant colleagues/senior management team about the alleged incident before searching a device

If there is an indecent image of a child on a website or a social networking site, then you should report the image to the site hosting it. Under normal circumstances, you would follow the reporting procedures on the respective website. However, in the case of a sexting incident involving a child or young person where you feel that they may be at risk of abuse, then you should report the incident directly to CEOP www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

STEP 3 - What To Do and Not To Do With The Image

If the image has been shared across a personal mobile device:

Always

- Confiscate and secure the device(s)

Never

- View the image unless there is a clear reason to do so
- Send, share or save the image anywhere
- Allow students to do any of the above
- If the image has been shared across a school network, a website or a social network:

Always

- Block the network to all users and isolate the image

Never

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in the Safeguarding and Child Protection policies and procedures.

STEP 4 - Who Should Deal With The Incident?

Often, the first port of call for a pupil is a class teacher. Whomever the initial disclosure is made to must act in accordance with the school Safeguarding and Child Protection policy, ensuring that the Designated Safeguarding Lead (DSL) and a senior member of staff are involved in dealing with the incident. The DSL should always record the incident. Senior Management should also always be informed. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first. If viewing the image is likely to cause additional stress, professionals should make a judgement about whether or not it is appropriate to do so.

STEP 5 - Deciding On a Response

There may be a multitude of reasons why a pupil has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion. It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere:

- Act in accordance with the **Safeguarding Policy and Child Protection Policy**, e.g. notify DSL/SMT team
- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make a referral to the Tri-borough Safeguarding and Child Protection officer LADO providing the incident that has taken place relates to a member of staff
- Contact the police (if appropriate)
- Put the necessary safeguards in place for the pupil, e.g. they may need counselling support, immediate protection and parents must also be informed
- Inform parents and/or carers about the incident and how it is being managed

(Depending on the nature of the image and the family circumstances of the young person, communication with parents will need to be carefully handled.)

STEP 6 - Contacting Other Agencies (Making a Referral)

If the nature of the incident is high-risk, consider contacting your local children's social care team. Depending on the nature of the incident and the response you may also consider contacting your local police or referring the incident to CEOP.

Appendix 5 : Keeping Children Safe Online At Home

General

The Dunham Trust recognises that the online world is largely a force for good but acknowledge the potential risks children face and some of the challenges that it poses. The aim of this policy is to help families enjoy the internet together as well as ensure that their children stay safe when they use the internet. The shifting landscape of technology means that the way children use it continues to change all the time. Handheld consoles, mobile phones, tablets, wristwatches and TVs are just some the devices that can be used to access the internet these days. This policy aims to provide parents with practical information and guidance that will assist them and other members of the Dunham Trust community in fulfilling the task of safeguarding children against possible harm online. The Dunham Trust recognises the potential harm that may be caused by a range of e-safety issues beyond the school boundary. These have been categorised into three areas of risks:

- **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**

In addition, the Dunham Trust understands the complexity of technology and e-safety matters in school and in the wider community. We have devised a set of guidelines to support families at home. School websites provide further advice and guidance and E-Safety workshops for parents are organised annually to continue to raise the profile of this important issue. The successful implementation depends on families following the guidelines below. The advice broadly covers all areas of social media that relate to children including gaming.

Pupils should follow these guidelines at home:

- I will be truthful about my age and recognise that social network sites have age limitations and that I will require parental permission to access these.
- I will only use my mobile devices, play games or use the computer with the permission of my parents'.
- I will not upload videos to the internet without my parents' permission
- I will not upload videos that contain images of pupils (including myself) wearing the NHP school uniform
- I will not upload any content to the internet without my parents' permission
- I will not use my full name when I upload videos to the internet; I may use an alias
- I will use the E-Safety sessions taught at school to help make decisions about how I behave online and offline

Gaming

Online gaming is an extremely popular pastime for people of all ages. One of its main attractions is that an online game may be played with a person or persons that live in a different city or country. There are many ways that games can be played online: there are free games, games that can be purchased, games on mobile phones and games that are played using handheld consoles and transmitted via a TV screen. Computer games are used at school to for learning. In promoting the health and wellbeing of its pupils, we recognise the value that may be derived from playing games offline and online in moderation. With this ideal in mind, we strongly recommend that the content, quality and quantity of video games to be viewed should be supervised by parents where possible.

The Dunham Trust strongly recommends that parents:

- Ensure that the use of games on mobile phones or consoles are included in the contract that you draw up with your child about internet use
- Ensure that parental age appropriate controls and settings are in place on all games consoles and devices that you use at home
- Create a shortcut on all devices to CEOP's report abuse button
- Follow the legal PEGI rating when purchasing games for your children
- Keep your own passwords secure
- Remember to sign out of any online accounts after any purchase is made online
- Know the purchasing options that exist for the games that you decide to buy i.e. iOS will require your Apple ID.

Pupils should follow these guidelines:

- I will let my parents help me decide who I can play games with online
- I will only play age appropriate games both on and offline
- I will use the E-Safety sessions taught at school to help make decisions about how I behave
- I will not use my full name when playing games with others on the internet
- I will not make 'In app purchases' without telling my parents that I am doing so
- I will only use purchase games with my parents' permission
- I will report abuse or things I find worrying to a trusted adult

The Dunham Trust recommends that you read the following documents where appropriate:

Read the parents guide to Instagram published by 'Connect Safely'
Read the parents guide to Snapchat published by 'Connect Safely'

Help your child to learn and follow the SMART rules:

Appendix 6: Reception /KS1 Computing Home School Agreement & Acceptable Use Agreement

Dear Parent/Carer,

Please read the following agreement with your child and sign below (they can also sign if they wish). This agreement is one of the ways that we promote e-Safety in school and ensure children understand how to use computers safely.

Regards

Computing Subject Leader

This is how we stay safe when we use computers:

I will ask a teacher or teaching assistant if I want to use the computers or an IPad.
I will only use activities that a teacher or teaching assistant has told or allowed me to use.
I will take care of the computer and other equipment
I will ask for help from a teacher or adult if I am not sure what to do, or if I think I have done something wrong.
I will tell a teacher or adult if I see something that upsets me on the screen.
I will use my class login when using the computer.
I will use the IPad with my number on.
I know that if I break the rules I might not be allowed to use a computer.

Name of child*:*_____

Signed (parent):_____

Appendix 7: KS2 Computing Home School Agreement & Acceptable Use Agreement

This agreement is to be read through with your parent(s)/carer. Unless it is signed and returned to school, Internet access will not be permitted.

- I must ask permission before accessing the Internet and I will not access other people's files.
- I will use my individual login or allocated I-Pad and understand I must not share these details with others.
- I will only e-mail people I know or that my teacher has approved and the messages I send will be polite and responsible.
- I will not respond to any messages that are mean or make me feel uncomfortable. If I do get any like that, I will tell my teacher immediately, so that the messages can be stopped.
- I will not give out my home address or telephone number, or arrange to meet someone over the internet.
- I must not look for rude or inappropriate materials on the World Wide Web. If I come across any such material by accident, I will tell my teacher immediately, so that further access to the site may be blocked.
- I will not bring in any programs on disc or CD ROM from home for use in school or download any program files to the computer from the Internet. (This is for both legal and security reasons).
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will handle school computing equipment with care and follow instructions given by the teacher.
- I understand that I may be denied access to the Internet if I do not follow these rules.

I have read through this agreement with my child and agree to these safety restrictions.

Name of child: _____

Signed: _____ (Child)

Signed: _____ (Parent/Carer)

Date: _____

Appendix 8: Anti-Cyber Bullying Policy

We believe cyber bullying is the use of a mobile phone or the internet to deliberately upset another person. We have a responsibility to ensure that cyber bullying does not take place in this school by ensuring pupils, school personnel and parents understand what it is and how it can be prevented.

We understand cyber bullying is highly intrusive and the hurt it causes can be very severe. As it leaves no physical scars cyber bullying is not easy to detect by a parent or a teacher.

We acknowledge cyber bullying can take place anywhere and can target pupils and school personnel. There are many types of cyber bullying such as text messages, picture/video clips, mobile phone calls, emails, chat room bullying, instant messaging and the use of websites to convey threats, intimidation, harassment etc.

We have a duty of care to protect pupils from cyber bullying as part of our responsibility to provide a safe, secure, caring and friendly school environment for all the children in order to protect them from those who wish to deliberately hurt them emotionally. We believe all our safeguarding procedures are in line with Sections 3(5) and 87(1) of the Children Act 1989 and Section 157 of the Education Act 2002 and that we promote the welfare of all children in our care.

We work hard to prevent cyber bullying by having in place a variety of safeguarding procedures.

We wish to work closely with pupils to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

Aims

- To ensure pupils, school personnel and parents understand what cyber bullying is and how it can be prevented.
- To have in place procedures to prevent incidents of cyber bullying.
- To have in place effective procedures to deal with all reported incidents of cyber bullying.
- To work with other schools to share good practice in order to improve this policy.

Responsibility for the Policy and Procedure

Role of the Governing Body - The Governing Body has:

- Appointed a member of staff to be responsible for ICT;
- Delegated powers and responsibilities to the Headteacher to ensure all school personnel and visitors to the school are aware of and comply with this policy
- Responsibility for ensuring that the school complies with all equalities legislation
- Responsibility for ensuring funding is in place to support this policy
- Responsibility for ensuring this policy and all policies are maintained and updated regularly
- responsibility for ensuring all policies are made available to parents
- the responsibility of involving the School Council in the development, approval, implementation and review of this policy
- nominated a link governor to visit the school regularly, to liaise with the Headteacher and the coordinator and to report back to the Governing Body
- responsibility for the effective implementation, monitoring and evaluation of this policy

Role of the Headteacher - The Headteacher will:

- Ensure all school personnel, pupils and parents are aware of and comply with this policy
- Work closely with the ICT coordinator to review how the school network is monitored
- Ensure the Acceptable Use Policy outlines how the ICT suite and the Internet should be used
- Provide support for those pupils and school personnel who may be victims of cyber bullying
- Deal with all incidents of cyber bullying quickly and effectively
- Work with parents in dealing with cyber bullying
- Distribute an information leaflet to parents outlining how they should monitor their child's use of the internet
- Inform parents of any incident of cyber bullying and how it has been dealt with
- Monitor the number of recorded incidents in an academic year
- Monitor the types of cyber bullying that occur in an academic year
- Monitor how swiftly incidents of cyber bullying are dealt with
- Discuss with the pupils

Are pupils aware of this policy?
How can cyber bullying be effectively dealt with?
How good are school personnel in dealing with incidents of cyber bullying?
How good are school personnel in identifying the symptoms of cyber bullying amongst pupils?

- Encourage any cyber bully to change their behaviour
- Impose sanctions on any pupil who continues to cyber bully
- Consider permanent exclusion in the most serious incidents of cyber bullying
- Consider the use of legal powers under the Education Act 2006 that allow him/her to regulate behaviour of pupils when they are off-site
- Provide leadership and vision in respect of equality
- Provide guidance, support and training to all staff
- Monitor the effectiveness of this policy
- Annually report to the Governing Body on the success and development of this policy

Role of the Computing Subject Leader - The subject leader will:

- Work closely with the Head of School to ensure that:
    - the Acceptable Use Policy is up to date
    - the school network is monitored
    - information is provided for pupils and parents
- Provide guidance and support to all staff
- Ensure cyber bullying is discussed during staff meetings and inset days
- Ensure cyberbullying is discussed with pupils through class discussions
- Invite pupils to consider the effects of cyberbullying
- keep up to date with new developments and resources
- review and monitor
- annually report to the Governing Body on the success and development of this policy

Role of the Nominated Governor - The Nominated Governor will:

- Work closely with the Head of School and the subject leader
- Ensure this policy and other linked policies are up to date
- Ensure that everyone connected with the school is aware of this policy
- Report to the Governing Body every term
- Annually report to the Governing Body on the success and development of this policy

Role of Staff - School personnel will:

- Comply with all the afore mentioned aspects of this policy
- Be alert to the dangers of cyber bullying
- Report all incidents of cyber bullying to a member of the Senior Leadership Team
- Ensure that no pupil has unsupervised access to the Internet
- Regularly remind pupils of:
    - the safe use of computing resources
    - the Acceptable Use Policy
    - the need to report any incident of cyber bullying to a member of the school personnel
- Inform pupils of the dangers of cyber bullying through PSHE, collective worship, anti-bullying week activities etc
- Be advised not to give their mobile phone numbers or email addresses to any pupil
- Be advised not to accept as a 'friend' any pupil on to their FaceBook page
- Seek the views of pupils in monitoring and evaluating this policy
- Implement the school's equalities policy and schemes
- Report and deal with all incidents of discrimination
- Attend appropriate training sessions on equality
- Report any concerns they have on any aspect of the school community

Role of Pupils - Pupils will:

- Comply with all the afore mentioned aspects of this policy
- Sign an Acceptable Use contract in KS2
- Be encouraged to report all incidents of cyber bullying to a member of the school personnel
- Not bring mobile phones to school unless they have prior permission from the Headteacher
- Listen carefully to all instructions given by the teacher
- Ask for further help if they do not understand
- Treat others, their work and equipment with respect
- Take part in questionnaires and surveys

Role of Parents - Parents will:

- Be made aware of this policy
- Comply with this policy
- Sign an Acceptable Use contract as part of the home school agreement
- Be encouraged to discuss the contract with their children
- Report all incidents of cyber bullying involving their child to the school
- Be asked to take part periodic surveys conducted by the school
- Support the school Code of Conduct and guidance necessary to ensure smooth running of the school

Recording and Reporting

- All reported incidents are investigated and dealt with
- Parents are informed of all events and what actions have been taken
- Records will be kept of all incidents and their outcomes

Dealing with Cyber Bullying Incidents

The Head of School will:

- Deal with all incidents of cyber bullying quickly and effectively;
- Impose sanctions as outlined in the school's Behaviour policy on any pupil identified as being the bully;
- Confiscate any mobile phone if brought to school;
- Contact the police and social services if the cyber bullying is sufficiently severe;
- Keep parents informed of the school's actions

Counselling & Support

Counselling and support mechanisms are in place to help those who have been bullied.
All perpetrators of bullying are given time to discuss why they have bullied and why their actions were wrong.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- The school website
- The Staff Handbook
- Meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- School events
- Meetings with school personnel
- Communications with home such as weekly newsletters and of end of half term newsletters
- Reports such annual report to parents and Headteacher reports to the Governing Body

Training

We ensure all school personnel have equal chances of training, career development and promotion.

Periodic training will be organised for all school personnel so that they are kept up to date with new information and guide lines concerning equal opportunities.

Monitoring and review

The implementation of this policy will be monitored by the Heads of School, who will make an annual report to the Local Governing Body of that school.

Approval by The Dunham Trust

Signed: _____
Date: _____
Review date: _____

This policy, signed by a Director on behalf of the Dunham Trust, is held centrally on the One Drive.

End of policy statement