EAST MORTON CE PRIMARY SCHOOL

Everyone, Every Chance, Every Day

bdat

Bradford Diocesan
Academies Trust

EAST MORTON CE PRIMARY SCHOOL

E-Safety Policy

Updated: Autumn 2019 CD

East Morton CE Primary School E-Safety Policy

The Internet and other technologies have the potential to offer many positive benefits to young people. As with everything, this is not without risk. We want young people to be able to fully exploit the benefits offered by computing while doing so in a safe manner. Online messaging, social networking and mobile technology effectively mean that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies.

In their e-safety guidance (September 2012) Ofsted states that the breadth of e-safety issues can be categorised into three areas of risk:

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

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school computing systems, both inside and outside of the school.
New technologies play an integral part to the lives of children both within and outside of school.

The internet and other digital devices are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to sage internet access at all times.

The uses of these new technologies within schools and at home have shown to raise educational standards and promote pupil achievement.
However, the use of these technologies can put children at risk within and outside the school. Some of the dangers may include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those that they make contact with on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

At East Morton CE Academy, we believe that it is essential, through good educational provision, to develop pupils' awareness of, and resilience to, the risks that they may encounter. We wish to arm children with the confidence and skills to recognise and deal safely with issues concerning their own, and others' E-safety. Through working with and supporting parents, we aim to ensure that this extends out of school too.

1. Development and Review

This e-safety policy has been developed by the E-safeguarding team made up of:

- Head Teacher – Mrs Kathryn Savage
- Designated Safeguarding Lead for E-safety – Mrs Emma Petts
- Deputy Safeguarding Lead with Responsibility for E-safety – Mrs Caroline Dewhirst
- Designated Safeguarding Lead for Early Years – Vicky Beecroft
- Safeguarding Team Member – Miss Shannen Marshall, Mr James Holland
- Executive School Business Manager – Mrs Suzanne Spencer
- Tech Support (Primary Technology) – Mr Matthew Dominik
- E-Safeguarding Governor – Mr Mike Isaac

Consultations with the whole school community have taken place through the following:

- Full staff meetings
- School council
- Full Governing Body Meetings
- School Website/Newsletters

The e-safety policy was approved by the teaching staff, leadership team and school Governing Body.	
The implementation of this policy will be monitored by the E-safety Team	
Monitoring will take place at regular intervals	Annually
The E-safety Policy will be reviewed annually or more regularly in the light of any significant new developments in the use of new technologies, new threats to e-safety or incidents that have taken place.	The next review Date November 2020
Should serious e-safety incidents take place the following external persons should be informed: Parents, CEOP/Police, Local Authority	Named persons in school: Mrs Petts and Mrs Savage

The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMs
- Internal monitoring data for network activity
- Pupil survey responses from E-safeguarding surveys completed within school

2. Roles and Responsibilities

Governors

Mike Isaac, chair of the Governing Body, has taken on the role as E-safety governor. E-safety is a standing item on Teaching and Learning Committee agenda and may include, when appropriate:

- Monitoring of E-safety Incidents via CPOMS

Head Teacher

- The Head Teacher is responsible for ensuring the safety of members of the school community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead for E-safety – Mrs Emma Petts, and Deputy Safeguarding Lead with Responsibility for E-safety – Mrs Caroline Dewhirst
- The Head Teacher is responsible for ensuring that the DSL, Deputy DSL for Esafety and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant
- The Head Teacher and another member of SLT (Mrs Petts) should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

Deputy Safeguarding Lead with Responsibility for E-safety

- Leads the e-safety team
- Takes a day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the schools e-safety policy
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with Local Authority
- Liaises with the schools computing technical team (Primary Technology)
- Receives reports of e-safety incidents and creates a log of incidents on CPOMs to inform future e-safety development
- Reports regularly to SLT

Teaching and Support Staff

Responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the e-safety team or named persons for child protection

Pupils

- Are responsible for using the school computing systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before gaining access to the school system
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Pupils understand and know how to use the safe search button and CEOP button on the desktop, website and blog
- Will be expected to know and understand the agreed AUP on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking /use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that they should apply the school's E-safety Policy outside school hours

Parents/Carers

Will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy

Technical Support (in house/Primary Technology/Smoothwall filtering and monitoring /Bradford BLN)

Will be responsible for:

- That the school's computing infrastructure is secure and is not open to misuse or malicious attack
- That they keep up to date with e-safety technical information to inform and update others as relevant

Smoothwall Monitoring Management will contact the Safeguarding Lead with Responsibility for E-safety and Deputy Safeguarding Lead with Responsibility for E-safety directly via a report regarding any issues of misuse

3. Training and Education

Training and Education - Pupils

E-safety education will be provided in the following ways:

- Planned e-safety teaching, embedded throughout the Purple Mash Scheme which is followed in school
- E- safety best practice is embedded at any time that technology is used in school
- Signed Class copies of pupil AUP will be displayed in classrooms
- Digital Leaders will have an understanding of whole school age appropriate activities regarding e-safety
- Opportunities are created to allow pupils to educate each other and their parents about E-safety

Training and Education – Parents/Carers

- Parents/Carers play an essential role in the education of their children and in the monitoring of children's on-line experiences
- The school will therefore seek to provide information and awareness to parents/carers through:
- Letter updates where required, the school weekly newsletter, the school website, and other support resources where appropriate

Training and Education – Staff

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

- The Lead and Deputy Safeguarding Lead with Responsibility for E-safety will participate in regular CEOP training and updates
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the schools e-safety policy and Acceptable Use Policies.
- The E-safety team will provide advice/guidance/training as required to individuals as required

Training and Education – Governors

- Governors will attend e-safety training; opportunities for further training will be reviewed. The E-safety team will provide guidance

4. Internet Use

The Internet is a communications medium that is freely available to any person wishing to send e-mail or publish a web site, and in common with other media such as magazines, books and videos, some of the material available is unsuitable for children. The measures outlined below are designed to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet.

Pupil's access to the internet is filtered via Bradford BLN (Bradford Learning Network) and Smoothwall Filtering. This should ensure that access is safe and secure, while protecting young users from abuse. The school works with Bradford BLN , Smoothwall (filtering and monitoring) and Primary Technology to ensure that the systems to protect pupils are subject to regular checks to ensure that filtering methods are appropriate, effective and reasonable. Parental permission is sought, and expectations of children are made clear, via the Pupil AUP, prior to children accessing the Internet or any other communication technologies.

Ensuring Safe Use

- Internet access provided by Bradford BLN (Bradford Learning Network), is a service designed for children including Smoothwall filtering system intended to prevent access to material inappropriate for children.
- Children using the Internet will be working in the presence of the class teacher or other approved adult helper
- Children conduct searches on 'Child Safe Sites' where possible such as: kidrex.org, swiggle.org.uk or safesearchkids.org
- If using a general search site (like Google), staff ensure pupils follow an agreed search plan (For example, children search only for words which have already been checked; or if new search terms are suggested, they are checked- away from the sight of the children- prior to permission to search them being granted)
- Staff will check that sites pre-selected for children's use are appropriate for their age and maturity
- Children are taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others
- Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils' acceptable use and risks

5. Blogging

Although blogging has been around for a number of years it has only been in the recent years that it has been used as an educational tool to give children a voice and an audience through blogging. This policy will outline the safe management of setting up and running a blogging platform.

A successful blog can:

- Safely give pupils a wider audience for their learning
- Encourage reluctant learners to participate and succeed in writing
- Allow pupils to receive feedback safely from different people all over the world
- Allow pupils to peer assess on each other's learning.
- Facilitate collaboration and shared learning across ages, contexts and cultures
- Encourage parental engagement

E-safety

Blogging involves pupils working on a blog whilst in school and also at home. Most blog platforms allow accounts to have different permissions. Contributor is the lowest level that allows a user to post. A contributor can submit a post for review; however, this will need to be authorised by the admin team before it appears on the blog. The contributor permission level is recommended for Primary School. Any other permission level above that of contributor will allow posts to be viewable as soon as the pupil clicks submit.

In the event of blogging projects in school, East Morton CE Primary School will seek permission for each child to have access to the school blog and to their learning and photographs displayed there. The child's full name will not appear alongside images of the pupils. Each child will have a computer generated avatar next to their post so individual photos are not used. Each pupil with a unique log in has be told to keep this private, if a pupil or parent thinks his or her log- in needs changing school must be contacted.

Blog Rules

Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risk and will ensure that users stay safe whilst blogging.

- Use only first names – No surnames
- Do not share you log in details – Keep them safe
- Keep safe – Do not reveal any personal information, or your location
- Write in good English – Including grammar and punctuation
- Be Polite – Do not post anything that could hurt anyone
- Always show Respect – Be positive if you are going to comment

Parents are very welcome to comment on our blogs, staff in school will moderate all comments before they go live on the blog. Parents are asked to adhere to the same rules as the children for blogging.

6. Data Protection

Technical Infrastructure, filtering and monitoring

- The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible
- School broadband is provided by Bradford BLN
- All internet activity is filtered and monitored by Smoothwall
- Primary Technology will ensure all antivirus protection is installed and updated
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to the school's computing system
- All users will be provided with a unique username and password for online services
- Computing team will keep a record of users and their usernames
- CPOMS is an electronic safeguarding monitoring system, in which staff members log incidents and record updates which alert members of the E-safeguarding/safeguarding team. This enables the careful monitoring and analysis of an incidents; allowing patterns and trends to be detected (and addressed) and reports to be generated for the E-safety Team/Governors as required

Use of digital and video images – Photographic and Video

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images; in particular, they should recognise the risks attached to publishing their own images online
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes at any time
- Photographs of children published on the website or blog must not contain the child's full names
- Pupils' full names will not be used anywhere on the school website or blog
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Staff Responsibilities - Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of all personal data, minimising the risk of its loss or misuse
- Do not store personal data offsite on laptops or memory sticks
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data
- Trackers and assessment of personal data must be stored onto T-drive or alternate secure drive on the school server with limited user access
- If extreme circumstance leads to secure data being stored on an external storage device (such as memory stick) it must be encrypted and securely password protected
- Use school email accounts for all professional communication

- Ensure that sensitive pupil information is not displayed to the class during registration/lunch registration or using CPOMS - screens are turned off or 'extended' to avoid any data breech

7. Communications Technologies

A wide range of communications technologies have the potential to enhance learning.
The official school email service is used for communications between staff, and with parents/carers and students, as it is regarded as safe and secure, provides an effective audit trail and is monitored.
The Acceptable Use Policies clearly outline how communication technologies, including e-mail, can be used to communicate across the school community and all users sign up to these and follow them. The school ensures that, where communication technologies are used then tools are chosen that enable staff to monitor their use, for example, moderated blogs, e-mail which can be monitored and secure areas for sharing information. This is sometimes through the use of group and class accounts for ease of monitoring.

The following table shows how the school allows communication technologies to be used.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices (school devices)		x					x	
Use of personal gaming devices		x					x	
Use of personal email addresses in school, or on school network	x							x
Use of school email for personal emails				x				x
Use of open chat rooms / facilities				x				x
Use of school limited chat facilities			x				x	
Use of instant messaging across the school community			x					x
Use of social networking sites		x						x
Use of moderated social networking sites only across the school community	x						x	
Use of blogs	x						x	
Use of moderated blogs only across the school community	x						x	

8. Staff Use of Social Media and computing

Introduction – Social Media

The school recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide range of social media. However, employees' use of social media can pose risks to confidentiality and intellectual property, the school's reputation and can jeopardise compliance with legal obligations.

While recognising the benefits of these media within the educational environment, in order to minimise the above risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate purposes, this section sets out the principles that all school employees must adhere to.

Employees must be conscious at all times of the need to keep their personal and professional lives separate.

This applies to all school employees (including teachers, support staff and trainees), is non-contractual and may be amended at any time. Breach of this policy may give rise to disciplinary action.

Staff Use – Social Media

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- You must not engage in activities involving social media which might bring the school into disrepute.
- You must not represent your personal views as those of the school on any social medium.
- You must not discuss personal information about pupils, other school employees or professionals you interact with as part of your job on social media.
- You must not use social media and the internet in any way to attack, insult, and abuse or defame pupils, their family members, colleagues, other professionals, other organisations or the school.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the school or the trust.
- You must ensure, when contacting students for school business, appropriate monitored resources i.e. school mobile phone, school email system etc are used as a safeguarding measure.

Staff Use – Social Media (Personal Use)

- **Employees must not identify themselves as employees of the school in their personal web space**. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.
- **Employees must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.**
- **Employees must decline 'friend requests' from pupils they receive in their personal social media accounts.** Instead, if they receive such requests from pupils of any school who are not family members, they may discuss these in

general terms in class where the pupils attend the school and signpost pupils to become 'friends' of the official school site if there is one.

- **Information employees have access to as part of their employment, including personal information about pupils and their family members, colleagues, trust staff and other parties and school or Trust corporate information must not be discussed on their personal web space**.
- **Photographs, videos or any other types of images of pupils and their families or images depicting employees wearing clothing with school logos on must not be published on personal web space.**
- **School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.**
- **Employees are advised that they set the privacy levels of their personal sites as strictly as they can** and to opt out of public listings on social networking sites to protect their own privacy. Employees should keep their passwords confidential, change them often and be careful about what is posted online. It is not appropriate to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Staff Use – Social Media (Professional/School Use)

Employees can only use official school sites for communicating with pupils or to enable pupils to communicate with one another.

- Employees should seek permission from the Head Teacher before creating an official school site explaining their business reasons for doing so.
- Any official school sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.
- Employees must, at all times, act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- If you are contacted for comments about the school for publication anywhere, including in any social media outlet please direct the enquiry to the Head Teacher.

Staff Use - School Computing Equipment

The computing and communications facilities within school are an important resource for teaching, learning and personal development and an essential aid to business efficiency. Staff are encouraged to take full advantage of the potential for computing and communications systems to enhance development in all areas of the curriculum and school administration. We recognise that along with these benefits, there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate material.

In addition to their normal access to the school's computing and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of computing equipment and email and internet facilities during their own time subject to such use:

1. Not depriving pupils of the use of the equipment and/or
2. Not interfering with the proper performance of the staff member's duties.

Staff who use the school's computing and communications systems, whether inside or outside of school must:

- Use school computing systems in an appropriate, courteous and responsible way
- Keep passwords confidential and must report any breach of password confidentiality Esafety Lead as soon as possible
- Consistently take all possible steps to adhere to the rules set out in the Staff and Visitor Acceptable Use Policy
- Must report any known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's Computing systems
- Recognise that any equipment provided to a school employee is provided for their sole use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.
- Report to the Head Teacher or designated safeguarding officer any vulnerabilities affecting child protection in the school's computing and communications systems
- Must not install software on the school's equipment unless authorised by the school's Esafety Lead, Office Manager or Technician
- Comply with any computing security procedures governing the use of systems in the school, including anti-virus measures
- Recognise that any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken

Staff Use - Email and Internet and Communications Systems Usage

Staff are required to use Email and Internet communications systems in line with their intended professional purpose only. These systems may not, under any circumstances, be used for the receipt, or distribution of, any inappropriate materials such as that which may bring the school into disrepute.

The forwarding of Chain Mail is prohibited and personal business or financial/political activities should be conducted elsewhere.

The SLT and the Governing Body can monitor and inspect staff use where misuse is suspected under the Regulation of Investigatory Powers Act 2000.

Refer to BDAT's 'Social Media Policy' for further detail relating to Section 8
The policy is available on the BDAT website:
http://www.bdat-academies.org/bdat-business/bdat-policies/

9. Reporting and Dealing with E-safety Incidents

There are activities that are inappropriate in a school context and users should not engage in these activities in school or outside school when using school systems.

We expect all members of the school community to be responsible users of computing, who understand and follow this policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, deliberate misuse.

School-based reporting processes are clearly in place and understood by the whole school. They are detailed in the Acceptable Use Agreements and are summarised as follows:

- Pupils report any issue to their teacher or other adult
- Staff are to follow the 'Actions for discovering Inappropriate or Illegal Material' Guidelines', which are kept within the Class File for each class. Overview of steps provided here.
    1. Remove the device from the sight of children. If it's a web site do not close any browser windows. Do not shut the device down.
    2. Preserve the evidence. If the image contains child abuse do not copy it. Take screenshots of the page in question **unless** the image involves child abuse.
    3. Inform the E safeguarding officer.
    4. Write the incident in the e safeguarding log as soon as possible.
- The E-safeguarding Team will deal with incidents in line with the 'E-safeguarding Officers Plan of Action' as detailed on table overleaf.
- Any issues that cannot be resolved by the E-safeguarding Team are escalated to involve the Head Teacher.
- The E-safety lead must report any issues to do with filtering to the E-ICT help desk.
- If any misuse appears to involve illegal activity, the Head Teacher will be consulted and reports to the Local Authority and police may be made. Particular reference to the rules around preservation of evidence will be made (i.e. preserve if appropriate only, do not reproduce/save inappropriate images).

Illegal activity could include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

- The E-safeguarding team are responsible for ensuring staff are kept fully informed about any issues and their resolution. Any incidents, and actions resulting are recorded using the CPOMs system.
- CPOMs is reviewed by the E-safeguarding Team to monitor new or ongoing risks and enable preventative action to be taken (in planning for E-safety Curriculum Coverage and Staff/Parental Awareness for example).

An E-Safeguarding Officer's Guide to Dealing with Referred Incidents.

Contact. A pupil has reported feeling uncomfortable after being contacted online. This may be through social networking, email, text, phone or by other means.	Exposure Exposure to inappropriate images, text and media. Including but not limited to nudity, porn, race hate material.	Bullying Aimed at staff/pupils/parents. Including but not limited to defamatory posts on social media sites, texts, MMS, sexting, frape. Phone calls, video conferencing	Inappropriate Behaviour. Including but not limited to: swearing, rude / insensitive comments on social media sites, email, texts.	Breach of Copyright Downloading and or use of copyrighted images, text, sounds and video.	Obsessive Behaviour This behaviour will usually take place away from the school site. It may involve playing games or chatting online for long periods of time.	Loss /theft of sensititve data. A laptop/ tablet/ usb stick has been lost/stolen or staff email/ school network has been accessed by non authorised personnel.
Inform the Headteacher immediately. The Headteacher will follow safeguarding guidelines and may contact the police or Bradford Council Safeguarding team as necessary. If the Headteacher is not present alert the alternative named child protection person. Preserve evidence of attempted contacted if available by taking screen shots and saving. Consult http://ceop.police.uk/safety-centre/ and consider reporting the incident to CEOP.	Has the staff member who discovered the incident…. • Isolated the device? • Preserved the evidence? • Written up the incident in the school (e) safeguarding log?	See all points in the Exposure. Column. ←	See all points in the Exposure. Column. ←	See all points in the Exposure. Column. ←	Obsessive behaviour may result in mood swings, being short tempered, withdrawal from friendship groups or drowsiness.	Report loss of equipment to the Headteacher.
	If you need to block sites or report issues with sites contact your broadband provider. The Bradford Learning Network number is 01274 385844 Make sure the device is removed to a place not accessible by children. Do not use the device until the full investigation is completed and detailed in the (e) safeguarding log. Consult named safeguarding/child protection person in school regarding further action Has there been a breach of the pupil AUP? Consult HT regarding possible sanctions. Has there been a breach of the staff AUP? Consult HT regarding possible sanctions. Has any illegal activity taken place? Consult HT with regards to contacting the Police. Write details of all follow up actions in the school e Safeguarding log. Fort further advice contact Bradford Council's Curriculum ICT team on 01274 385844	Advice. Notify parents. Do not respond to posts/ calls/texts. Contact social media sites and ask them to remove posts. Report abuse to phone network. Tell a trusted adult every time a call occurs and keep a record. Record an image of any further abuse. Consider asking the poster to remove the material and teach them about the impact of their actions. Consider adapting content of PHSCE / SEAL lessons and assemblies to address the problem. Teachers who have been abused online can contact the UK Safer Internet Centre on 0844 381 4772 or email helpline@saferinternet.org.uk	Advice. Notify parents. Consider adapting content of PHSCE / SEAL lessons and assemblies to address the problem. Check logs of user activity on devices to identify phrases that were typed. This could be Smoothwall logs or other monitoring systems used in school such as E Safe or Policy Central.	Advice. Notify parents. Do staff need training in the location, use and attribution of material? The Research strand of Bradford Council Curriculum Innovation Team's ICT scheme of work covers copyright and attribution of sources. Lists of sites with copyright free/ creative commons images and sound can be found at http://innovationcentres.org.uk/ go to Curriculum > Primary > Sound and Music or Multimedia.	Advice Discuss child's behaviour with relevant staff in school, class teacher, learning mentor. Invite parents / carers in to discuss the situation. Offer advice regarding excessive gaming. See the parent section at www.thinkuknow.co.uk Consider running parental advice sessions. The presentation for parents can be found in the teachers section of www.thinkuknow.co.uk. It can be delivered by teachers who have registered at the site.	Contact the Police if property has been stolen. Speak to the relevant administration personnel in school regarding contacting insurers. Create a list of all password protected services on the device. Change all passwords. If person information was lost consider informing those people affected.

Please read in conjunction with:

- Computing & Computing Policy
- PHSE Policy
- Safeguarding Policy
- Staff/Visitor Acceptable Use Policy 2019
- Pupil's Acceptable Use Policy 2019
- BDAT's Social Media Policy http://www.bdat-academies.org/bdat-business/bdat-policies/

Headteacher:

Governor Approval:

Date: 28th November 2019