Designated Child Protection/ Safeguarding Officers: James Mobbs, Andrew Velasco, Vanessa Cornish

Date Policy Approved – 11/05/10 **Reviewed –** MichaelmasLent 20187

Next Review – MichaelmasSummer Term 202018

1. INTRODUCTION

The Department for Education published the revised statutory guidance 'Keeping Children Safe in Education' (KCSIE September 20186). Among the revisions, schools are obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over-blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Schools in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self-review systems (eg www.360safe.org.uk) that will support schools in assessing their wider online safety policy and practice.

This e-Safety Policy is part of the school's safeguarding policy. This policy relates to other policies including the Code of Conduct for Staff, *Anti-Bullying and Child Protection Policies*. The policy has been developed in light of a review of our organisation's safeguarding practice in the use of a major technology and its benefits and risks. Staff, parents, carers and young people themselves are involved in deciding the policy. We believe that we provide a caring, positive, safe and stimulating environment where children can develop.

This school fully recognises the responsibility it has to the safeguarding and protection of children and young people who use our service. All staff members, including volunteers, have a full and active part to play in protecting children and young people from harm.

This policy should cover the responsibility of agencies to safeguard children from harm, responding to and investigating incidents, protecting staff, storing information securely.

2 AIMS

- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupils or liability to the school.
- Raise awareness and understanding of e-safety issues amongst children and young people where they are using the school's equipment.
- Ensure that staff understand the importance of e-safety in safeguarding and develop their understanding of the signs and indicators of abuse.
- All members of staff are aware of actions required to assist a child or young person who reports e-abuse.
- Know how to report online abuse.
- All staff know how to respond to a young person who discloses abuse.
- Establish safe access to the internet for children and young people
- Provide a systematic means of monitoring children known or thought to be at risk of harm.
- To ensure that all adults who have access to children's information have been checked as to their suitability and have an enhanced CRB disclosure, as well as a List 99 check.

3. PROCEDURES

We will ensure that:

- We have a Designated Safeguarding Lead (DSL) who will, in line with recommendations in the Keeping children safe in education September 2016 undertake training and refresher training.
- The school has in place an acceptable use policy for the use of internet or other online equipment.
- All members of staff develop their understanding of the signs and indicators of digital abuse or need through training
- All pupils receive e-safety training that is appropriate to their age.
- All members of staff know how to respond to a child who discloses digital abuse.
- All parents/carers will be made aware of the organisation's Child Protection/Safeguarding Procedures, e-safety policy, and will be given advice on e=safety at home
- All staff members are responsible for reporting concerns regarding a colleague's behaviour. *See Whistle-blowing Procedures.*
- This procedure will be regularly reviewed and up-dated.
- All staff will have seen a copy of this policy and new staff will be given a copy as part of their induction programme.

3.1 Responsibilities

This policy was prepared by the Designated Safeguarding Lead.

This e-Safety Policy was agreed by the senior management team and staff.

The e-Safety Policy and its implementation will be reviewed annually.

3.2 The role of the Designated Safeguarding Lead

The Designated Safeguarding Lead is responsible for:

- Adhering to the *London Child Protection Procedures September 2016*, *Bromley Safeguarding Children Board and organisation's policies* with regard to referring a child if there are concerns about possible abuse.
- Keeping a written record of concerns about a child even if there is no need to make an immediate referral.
- Ensure all records are kept confidentially and secure and are separate from other records related to the child.
- Raise awareness on digital communication safety.
- Ensure that children and young people are aware of how/where they can report abuse.

The designated teacher must access appropriate training.

4 THE DIGITAL TECHNOLOGY AS A RESOURCE?

4.1 Benefits

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet and mobile technology. Benefits of using the Internet:

- access;
- inclusion ;
- educational and cultural exchanges;
- vocational, social and leisure use;
- professional development for staff through access to national developments, materials and effective practice.

All young people need to learn to evaluate everything they read, hear and view and to refine their own communications with others via the Internet.

- *Young people will be advised on what Internet use is acceptable, what is not and given clear objectives for Internet use – Internet permission E SMART rules are given out to every new child, signed and returned to be held on file.*
- *Internet access will be planned to enrich and extend learning activities.*
- *Access levels will be reviewed to reflect the project requirements and young person's age.*
- *Staff should be available to provide guidance. Children will not be able to access the Internet unsupervised.*

4.2 Evaluate Internet content

Young people should be helped to understand what to do if they experience material that they find distasteful, uncomfortable or threatening.

Key information handling skills include establishing the author's name, date of revision and whether others link to the site.

Children and staff need to know how to deal with any Cyber Bullying incidents. Pupils need to know about the national agencies, such as Child Exploitation Online Protection (CEOP), http://www.ceop.gov.uk/ – so that in an extreme case, they know how to "report abuse".

5 MANAGING INFORMATION SYSTEMS

5.1 How will information systems security be maintained?

It is important to review the security of the whole system in terms of the personal safety of children and young people. ICT security is a complex matter and cannot be

dealt with adequately in this document. A number of agencies can advise on security including Becta and network suppliers.

The security of the organisation's information systems will be reviewed regularly.

Virus protection will be updated regularly.

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal data, other than progress reports currently being prepared by and relevant to staff, should not be held on portable media without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in " work areas or attached to e-mail.
- Files held on the organisation's network will be regularly checked.
- Filtering systems will be regularly maintained

5.2 User policies

This school:

- Will provide guidance on users acting reasonably
- Requires all staff and pupils to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Is vigilant when conducting 'raw' image search with young people e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and young people that that they must report any failure of the filtering systems directly to the ICT teacher and/or SMT.
- Ensures that our systems administrators report to SMT where necessary;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the school/ club / organisation.
- Makes information on reporting offensive materials, abuse / bullying etc available for young people, staff and parents;
- Immediately refers any material suspected to be illegal to the appropriate authorities – Police – and the LA.

5.3 Publishing material

The use of images and taking of video or photographs of children and young people requires parent/carer consent.

Young People need to be made aware of the reasons for caution in publishing personal information and images in social publishing sites. BSCB publish guidance on the safeguarding implications of the use of photographic and other images.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Work can only be published with the permission of the child and parents.

Tips for keeping safe on line:

- Young people will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Young people should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or his/her location e.g. house number, street name or school.
- Staff official blogs or wikis should be password protected and run from the school website. Staff should be advised not to run social network spaces for young people's use on a personal basis.
- Young people should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others.
- Young people should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

6 PROTECTING PERSONAL DATA

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Organisation will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

Possible statement:
Only individuals who have been CRB/DBS checked will have access to children's files.

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

7 DEALING WITH E-SAFETY SAFEGUARDING COMPLAINTS

Parents, staff and young people should know how to submit a complaint about a digital safeguarding issue and be aware of the report abuse button available on many sites. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside the organisation.

- Where an allegation is made against a member of staff, the Bromley *Procedure on Child Protection Allegations against Staff* needs to be followed.
- Child protection or illegal issues must be referred to the school Designated Child Protection Officer.
- Advice on dealing with illegal use could be discussed with the local Police Public Protection Desk.

8 REFERENCES

You can access the London Child Protection Procedures and Bromley safeguarding children procedures and policies via the Bromley Safeguarding Children Board website: http://www.bromleysafeguarding.org/documentdetails.asp.

Information Commissioner's Office: **http://www.ico.gov.uk/**

9 MAKING A CHILD PROTECTION REFERRAL

Referral & Assessment Team - West
Yeoman House, 4th Floor, 57-63 Croydon Road, Penge, London SE20 7TS
020 8461 7050
Monday - Thursday 8.45am-5.00pm
Friday 8.45 – 4.45pm

Referral & Assessment Team – East
The Walnuts, High Street, Orpington, BR6 0UN
020 8461 7379
Monday - Thursday 8.45am-5.00pm
Friday 8.45 – 4.45pm

Out of Hours – Emergency Duty Team
020 8646 4848
Monday to Thursday 5.00pm – 8.45am
Weekends and Bank Holidays 5.00pm – 9.00am the next working

Seek advice from a social worker if you are unsure whether to make a referral.

All referral should be sent using the multi-agency referral form. The exception is in the case of urgent child protection, where the referral will be taken over the telephone and followed up in writing by the next working day (24-72 hours).

With few exceptions the parents should be informed a referral is being made. If you are unsure consult a Duty Social Worker prior to sending the referral.

Common Assessment Framework
The CAF is designed as an assessment tool to facilitate early intervention and co-operation between agencies to improve outcomes for children/young people with additional needs.

You might use a CAF:

- If you are concerned about how the child is progressing in terms of their health, welfare and behaviour.
- You receive a request from the child/ young person or parent/carer for more support.
- You are concerned about the child/ young person appearance or behaviour but their needs are unclear or are broader than your service can address.
- To help you identify the needs of the child/ young person and /or to pool knowledge and expertise with other agencies to support he child/ young person.

CAF Team contacts:0208 461 7174.

Supporting, Monitoring and evaluating the effectiveness of the implementation of this policy - How is this done?

Visits from NSPCC who deal with online safety and bullying in workshops every other year for years 5&6

Online safety links on an internet safety page for children on the website

Online safety links on an internet safety page for parents on the website

Smoothwall filtering system on all computers used regularly by children

Regular discussions and planned lessons for children on internet safety with the teacher of Computing

Training - 

http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew/watch-full-movie

In addition, the CEOP Thinkuknow clips are also utilised.

The Computer teacher hosted online safety sessions for parents in March 2016.

Feedback to all staff after James Mobbs attended conference – Keeping Children Safe in a Digital age