ESAFETY POLICY

APRIL 2018

ASPIRE ACADEMY BEXLEY

ENDEAVOUR ACADEMY BEXLEY

HORIZONS ACADEMY BEXLEY

CONTENTS

ETHOS

The Academy recognises new technologies have become integral to the lives of children and young people in today's society, both within the academy and in their lives outside academy. ICT and the internet are fantastic tools for learning and communication that can be used in the academy to enhance the curriculum, challenge students, and support creativity and independence. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and young people learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. The use of these exciting and innovative tools in academy and at home has been shown to raise educational standards and promote student/student achievement.

Using ICT to interact socially and share ideas can benefit everyone in the academy community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. However, the use of these new and developing technologies can put young people at risk within and outside the academy. As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision, to build young people's resilience to the risks (to which they may be exposed) so that they have the confidence and skills to face and deal with them. We also recognise that there is the potential for excessive use which may impact on the social and emotional development and learning of the young person and it is important that all members of the academy community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm can include sending hurtful or abusive texts and emails, attempts to radicalise via the internet and social media enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any person working with children and the risks and responsibilities of e-safety fall under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in our academies and to provide a good understanding of appropriate ICT use that members of the academy community can use as a reference for their conduct online outside of academy hours.

E-safety is a whole-academy issue and responsibility. Cyber-bullying by students/ staff will be treated as seriously as any other type of bullying and will be managed through our behaviour and disciplinary procedures.

1. ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and Groups within our Academies;

New Horizons Academies Network & MIS Manager:
Mr Jon Hanson

Endeavour Academy E-Safety Coordinator is:
Beverley Evans Head of School

Aspire Academy E-Safety Coordinator is:
Heather Hopkins Deputy Headteacher

Horizons Academy Bexley E-Safety Coordinator is:
Ian Cooper Head of ICT

Designated Governor responsible for E-Safety is:
Corinne Botten Chair of Governors

Governors and their Boards are responsible for the approval of the E-Safety Policy and Governors are responsible for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents via the HT's report, monitoring reports throughout the academic year. A designated member of the Governing body has taken on the role of E-Safety Governor and their role will include:

- regular liaison with the E-Safety Co-coordinator
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering/change control logs
- providing feedback to Governing Body and Board Meetings

THE ROLE OF THE NETWORK MANAGER WILL INCLUDE:

- A duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Headteacher and E-Safety Co-coordinator.
- Ensuring the Headteacher and Senior Leaders are aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff.
- Ensuring that the Headteacher and the Designated Safeguarding Leads and E-Safety Co-ordinator and all other members of staff receive suitable training to enable them to carry out their e-safety roles.
- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets required safety technical requirements and any National E-Safety Guidance that may apply
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed
- Ensuring that the filtering policy is applied
- Ensuring that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as required

- Ensuring that the use of the network / internet / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported
- Ensuring that monitoring software / systems are implemented and updated

THE ROLE OF THE E-SAFETY CO-COORDINATOR WILL INCLUDE:

- taking day to day responsibility for e-safety issues and having a leading role in establishing
- and reviewing the school e-safety policies and documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of
- an e-safety incident taking place providing training and advice for staff liaison with Network Manager and 3rd party IT contractors receiving reports of e-safety incidents and creating a log of incidents to inform future esafety developments meeting regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Reporting when necessary to the Senior Leadership team.
- ensuring that they keep up to date with e-safety technical information in order to effectively
- carry out their e-safety role and to inform and update others as relevant

TEACHING AND SUPPORT STAFF ARE RESPONSIBLE FOR ENSURING THAT:

- they attend annual E-safety and Safeguarding Training sessions
- know who their Designated Safeguarding Lead and E-Safety Co-ordinator is
- they read and understand all guidance provided to them as part of training
- that they report any suspected misuse or problem to the E–Safety Co-coordinator and/or Designated Safeguarding Lead for next steps
- all digital communications with students/parents/carers will be on a professional level and only carried out using school systems – never on a personal device.
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the E-safety Student Agreement
- students have a good understanding of research skills and the need to avoid plagiarism and
- uphold GDPR
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices in lessons where internet use is pre-planned students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Leads are trained in E-Safety issues and are aware of the potential serious issues to arise both in the academy in and in the wider community, from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting

We acknowledge these points are areas of safeguarding and are formally recognised in, but not limited to the Safeguarding Policy. As part of this acknowledgement, all staff and Designated Leads share and respond to all safeguarding concerns following the process outlined in our Safeguarding Policy.

STUDENTS

- are responsible for using the Academy digital technology systems in accordance with the Student Agreement
- to adhere to Behaviour Policy
- have an 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
- will be expected to know and understand Academy rules on the use of mobile devices as outlined in the Behaviour Policy
- will be expected to know and understand Academy rules on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good E-safety practice when using digital technologies outside of Academy time and realise that the Academy's E-Safety Policy covers their actions out of school, if related to their membership of the Academy.

PARENTS/CARERS

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Our Academies will take every opportunity to help parents/carers understand these issues through parents' events, leaflets, letters, website, Parent Agreement and information about national / local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school
- their student's personal devices in the school

2. COMMUNICATING THE POLICY

This policy is available in each Academy site reception for visitors, website and from any Academy main office on request for parents/carers, staff, and students to access. Rules relating to on-line behaviour and e-safety guidelines are displayed around each Academy. E-safety is integrated into the daily curriculum within all our Academies where the internet or technology are being used and during PSHE lessons where personal safety, responsibility, and/or development are being discussed. Discussions relating to E-Safety policies and procedures should not and are not only limited to formal PSHE lessons or dedicated curriculum time as E-Safety is considered a natural part of daily communication by staff to students and forms part of duty of care in relation to safeguarding the students.

Parents and carers play an essential role in the education of their children and in the monitoring/supervision of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities, E-Safety Student/Parent Agreement, website and specific events and campaigns e.g. Safer Internet Day. We will also endeavour to provide signposting to any parents/carer or student who requires additional support and guidance.

3. TRAINING

STAFF

It is essential that all our staff receive E-Safety training and understand their responsibilities in relation to keeping children safe in education. Training enables our staff to feel confident and able to respond appropriately to any concerns or questions raised by either child or adult. Training will be offered to staff and Governors as follows:

- annually for all staff by external recognised providers
- all new staff will receive e-safety information as part of their induction programme, directing them to read and sign the school's E-safety policy, Codes of Conduct, GDPR and Safeguarding Policy including Keeping Children Safe in Education 2017
- inset days and in staff meetings when required
- E-Safety updates will be presented via weekly staff bulletins.
- the E-Safety Co-coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations including LSCB

GOVERNORS

Governors will be invited to take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- attendance at external training courses
- participation in Academy training/information session for staff or parents
- receipt of weekly staff bulletin

4. MAKING USE OF ICT AND THE INTERNET IN SCHOOL

ICT is used in learning to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance our Academies management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school therefore reducing the risk of them becoming NEET (not in education, employment or training). Some of the benefits of using ICT in education are:

FOR STUDENTS:

- Unlimited access to worldwide educational resources and institutions such as art galleries,
- Access museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between students all over the world.
- Access to subject experts, role models, inspirational people and organisations.
- The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

FOR STAFF:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

FOR PARENTS:

The majority of communication between our Academies and parents/carers is via telephone in person, however email and letters will also inform parent/carers of details relating to attendance, transport and behaviour. This provides both an alternative form of communication and validation of process implemented and purpose.

5. LEARNING TO EVALUATE INTERNET CONTENT

With so much information available online it is important that our students learn how to evaluate internet content for accuracy and intent. This is approached by individual Academies as part of digital literacy across all subjects with their curriculum.

Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright.

Our students are also educated through the curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the Academies network or their personal account or wellbeing.

At Endeavour Academy PSHE in Key Stage 3 and Key Stage 4 topics cover Internet Safety, How to stay safe, On-line Bullying, Radicalisation, Positive Relationships and Social Media. Evidence is through classroom discussions and work completed. This also forms part of the Key Stage 4 PSHE qualification which has a section for Personal Safety, where E-Safety is covered.

Aspire Academy have an e-safety unit within their Computing Scheme which is taught to all year groups. Cyber bulling is also covered in the PSHE Scheme of work with both feeding into the Long Term Curriculum Plans. Aspire Academy also facilitates an E-Safety Day annually where the learning is focused on keeping themselves safe on-line. All classes also have E-Safety display in their classes to provide visual cues.

Horizons Academy Bexley, E-safety is underpinned by ThinkUKnow and feeds into a variety of topics within PSHE programme, including healthy relationships, emotional wellbeing, personal safety, financial safety and more. Horizons Academy Bexley also facilitates an E-Safety Day annually where the learning is focused on keeping themselves safe on-line within tutor time.

Plagiarism is against the law and each Academy will take any intentional acts of plagiarism very seriously. Students who are found to have plagiarised will managed in line with the Behaviour Policy. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

Our Academies will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the Academy's Network Manager. Any material found by members of the Academy community that is believed to be unlawful will be reported to the Head of School and any appropriate agencies immediately. This behaviour may also be reviewed in line with HR policies and procedures and could be deemed a disciplinary matter.

6. MANAGING INFORMATION SYSTEMS

The Network Manger is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of our Academies data and personal

protection of the Academy community, very seriously. This means protecting the Academy networks as far as is practicably possible, against viruses, hackers and other external security threats. The security of the Academies information systems and users will be reviewed regularly and virus protection software will be updated regularly.

Some safeguards that our Academies take to secure our computer systems are:

- Making sure that unapproved software is not downloaded to any Academy computer.
- Files held on the Academy's network will be regularly checked for viruses ; Antivirus software is installed on all Academy PC's
- the use of user logins and passwords to access the Academy network will be enforced
- Portable media (USB sticks, CDs, etc.) containing school data or programmes will not be used under GDPR guidance

*For more information on data protection, please refer to our Data Protection Policy (GDPR).

7. E-MAILS

Our Academies use emails internally for staff and students and externally for contacting parents and other agencies. This is an essential and necessary part of our Academies form of communication. It is also used to enhance the curriculum by:

- Providing immediate feedback on work, and requests for support where it is needed.
- To provide parents with student absence information
- To all parents to make contact when they are not able to access the telephone

Staff and students must be aware that each Academy email accounts must only be used for Academy related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality and the maintenance of GDPR. The Academy has the right to review all emails and their contents at their discretion but will only do so if it feels there is a justifiable reason to do so.

7.1 USE OF BCC, CC AND REPLY TO ALL

Staff using email should ensure that they are aware of the difference between BCC and CC and that caution is used when "replying to all" to ensure that information is not shared accidentally with those not relevant. Information should only be shared in the best interest of the student.

7.2 SCHOOL E-MAIL ACCOUNTS AND APPROPRIATE USE

Staff should only use our official email accounts relative to each Academy, to communicate with students, parents or carers. Staff should not use official Academy provided email accounts for personal communications. Personal email accounts should not be used to contact any of these people for school business. The forwarding of chain messages is not permitted within any of our Academies.

Emails sent from each Academy accounts should always be professionally and carefully written. Staff must remember they are representing our Academies at all times and should take this into account when entering into any email communications. If staff should receive an email externally which they deem either inappropriate, offensive, threatening or unprofessional they should discuss with their manager in the first instance to confirm the next steps. If a staff member receives an email from an internal member of Academy staff, they should not respond. Staff should print the email and immediately share with their Line Manager. The Line Manager and staff member will decide the next steps in line with the Staff Code of Conduct and HR policies and procedures. If the staff member is not satisfied with the next steps relating to internal or external emails, then the Head of School or Executive Headteacher should be notified. They should not attempt to deal with the matter themselves or respond via email.

8. PUBLISHED CONTENT AND WEBSITES

Our Academy websites are viewed as useful tools for communicating our ethos and practice to the wider community and partnership agencies. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with our different Academy news and events, celebrating whole-school achievements, personal achievements, and promoting school projects.

Our website is in the public domain and can therefore be viewed by anybody online. Any information published on the websites will be carefully considered in terms of safety for the school community, copyrights and privacy policies and will comply with GDPR. No personal information on staff or students will be published and details for contacting our Academy individually will be via the main office only.

8.1 POLICY AND GUIDANCE OF SAFE USE OF STUDENT'S PHOTOGRAPHS AND WORK

Photographs and students work bring our Academies to life, showcase our student's talents, and add interest to publications both online and in print that represent all our Academies. However, we acknowledge the importance of having safety precautions in place to prevent the misuse of such material. Our Academies believe that celebrating the achievement of our students is an important part of their learning experience and personal development. Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community. However, we would also like to use photographs and videos of the Academies and its students externally for promotional purposes (in the public domain) and to promote the good educational practice of the Academies. However, in accordance with the Data Protection Act 1998 we will only do this with parent/carer consent. On admission to one of our Academies parents/carers will be asked to sign a Home School Agreement which incorporates digital/video permissions. By signing this form parents/carers will be consenting to the use of images of their child being used in the following outlets:

- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects

The form covers consent for the duration of the child's time with an Academy, however should a matter of safeguarding arise then consent can be rescinded by either party. Once the student leaves the Academy, photographs and videos will be archived within the Academy and will not be re-published without renewed consent. Consent will be gained directly with the student if over the age of 16 years. Students' full names will never be published externally with their photographs, but may be published internally (for example, on display with their work). A students' address will not be displayed either internally or externally.

USING PHOTOGRAPHS OF INDIVIDUAL CHILDREN

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, therefore as part of responsibility outlined in Keeping Children Safe in Education, we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. Only images created by or for our Academies will be used in public and children may not be approached or photographed whilst in an Academy school or doing school activities without the school's permission. Any member of the public or staff taking unauthorised photographs will be referred to the appropriate agencies and may also face formal HR process.

Our Academies follow general rules on the use of photographs of individual students:

- Parental consent must be obtained for external/promotional use.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This
- includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities) will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or class name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only and not be posted on any social media sites.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or in which they are being asked to participate.

Any photographers that are commissioned by the Academies will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times and will not have unsupervised access to the students and will abide by guidelines as per Safeguarding Policy.

8.2 COMPLAINTS OF MISUSE OF PHOTOGRAPHS OR VIDEO

Parents/ carers should follow the standard school complaints procedure, as outlined in our Complaints Policy which is accessible via the website, if they have a concern or complaint regarding the misuse of school photographs.

Parents/carers are advised to contact the Head of School directly regarding concerns relating to unofficial photographs in the Academy, during an activity, around an Academy perimeter or whilst travelling to and from the school day to ensure the wellbeing of all our students is maintained.

8.3 SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

Personal publishing tools include blogs, wikis, social networking sites, Skype, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the Academies expectations regarding the use of ICT and technologies and behaviour online.

Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use. Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use. Official Academy blogs is created by the Network and MIS Manager is password-protected and run with the approval of the Executive Headteacher and will be moderated in partnership with each other. Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful

or defamatory which may result in external agencies being notified including the Police. The Academies expect all staff and students to remember that they are representing the Academy at all times and must act appropriately. Safe and professional behaviour of staff online will be discussed at staff Safeguarding training and outline in relevant policies including but not limited to the Staff Code of Conduct. Staff suspected of operating outside of our policies and expectations may lead to formal HR process, disciplinary action and potentially dismissal.

9. MOBILE PHONES AND PERSONAL DEVICES

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged or lost
- they can have integrated cameras which can lead to safeguarding, bullying and data protection issues.

The Academies therefore do not allow mobile devices to be used by students during the school day and all students are expected to hand in all devices at the start of the school day as outlined in the Behaviour Policy. Devices will be returned at the end of the school day or at the completion of detention or make up time. If a student is leaving Academy site during the school day with consent e.g. unwell or following a fixed term exclusion then mobile devices will be returned as the student exits the site. Should a student decide to leave the Academy site without consent all mobile devices must be collected by parent/carer as soon as practicably possible.

In circumstances where there is a suspicion that material on a device/phone is possibly illegal or in connection with illegal acts, the device/ phone will be handed to the Police for further investigation as dictated within the Behaviour Policy under section Screening, Searching & Confiscation.

EMERGENCIES

If a student needs to contact his parents/carers they will be allowed to use an Academy phone at the discretion of the Senior Leadership Team and in line with the Behaviour Policy.

If parents/carers need to contact their child urgently they should phone the relevant Academy office and a message will be relayed appropriately to not impact on the smooth running of the Academy or disrupt the learning of others.

Endeavour Academy, Aspire Academy and Horizons Academy Bexley accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in/confiscated. Our Academies will not investigate theft, loss or damage relating to phones/devices.

Under no circumstances should staff use their own personal devices to contact students or parents either in or out of Academy time unless in an emergency. Our staff are not permitted to take photos or videos of students on their own devices. If photos or videos are being taken as part of the curriculum or in a professional capacity, the Academy equipment must be used. We expect staff to lead by example. Personal mobile phones should be switched off or on 'silent' during the school day. With the authorisation of the relevant member of the senior leadership team, some teams may use their personal mobile phones to make calls, texts or WhatsApp group in order to ensure effective communication or to ensure student or staff safety.

Any breach of policy may result in disciplinary action against that member of staff.

10. CYBERBULLYING

Cyberbullying, as with any other form of bullying, is taken very seriously by all the Academies. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the Anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all students and staff within our Academies what is expected of them in terms of respecting their peers, members of the public and staff and any intentional breach of this will result in consequences outlined in the Behaviour Policy for students and all related policies including the Staff Code of Conduct in relation to staff members.

If an allegation of cyberbullying (bullying) does arise, the Academy will:

- take it seriously
- act as quickly as possible to establish the facts.
- it may be necessary to examine Academies systems and logs or contact the service provider in order to identify the bully
- record and report the incident to all necessary agencies
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated.
- follow the Behaviour Policy
- follow HR processes

If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another (peer on peer), either physically or emotionally, redress their actions and the Academy will make sure that they understand what they have done and the impact of their actions. Restorative Approach will be adopted where appropriate and sanctions issued will be in line with the Behaviour Policy if required.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended and external agencies including the Police may be informed at the discretion of the Academy.

Repeated bullying may result in a fixed-term exclusion or disciplinary action.

11. MANAGING EMERGING TECHNOLOGIES

Technology is progressing rapidly and new technologies are emerging all the time. The Network Manager, in liaison with E-Safety coordinator and Heads of School will risk-assess any new technologies and consider any educational benefits before they are allowed into any of our Academies. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments. Heads of School undertake the 360 Degree Online Safety Review Toolkit (360safe.org.uk) twice per academic year and share the outcomes with their staff.

12. PASSWORD SECURITY

Many our systems for staff and students require the use of a password. All staff and students are supported to adhere to the following password guidelines:

- Never write passwords down.

• Never send a password through email.
• Never tell anyone your password.
• Never reveal your password over the telephone.
• Never hint at the format of your password.
• Don’t auto save passwords e.g. in a browser.
• Never reveal or hint at your password on a form on the internet.
• Report any suspicion of your password being broken to the Network & MIS Manager.
• Don't use common acronyms as part of your password.
• Don't use common words or reverse spelling of words in part of your password.
• Don't use names of people or places as part of your password.
• Don't use part of your login name in your password.
• Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
• Be careful about letting someone see you type your password.
• **Staff should ensure that they lock their computer, even if leaving it for a short time, and that they log off at the end of a session.**

13. UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or disturbing racist material is illegal and is banned from all our Academies and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an Academy context, either because of the age of the user or the nature of those activities. The following activities would be inappropriate in our context:

- pornography
- promotion of any kind of discrimination and radicalisation
- threatening behaviour, including promotion of physical violence, torture ,mental harm and
- FGM
- any other information which may be offensive to colleagues or breaches the integrity of the
- ethos of the schools or brings the schools into disrepute
- using Trust/school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by our Academies
- infringing copyright
- revealing or publicising confidential or proprietary information e.g. financial, personal information, data bases, computer / network access codes and passwords
- creating or propagating computer viruses or other harmful files
- unfair usage, downloading or storing information for personal use
- non-educational on-line gaming, on-line gambling
- use of social media without permission
- use of messaging apps without permission
- use of videoing broadcasting or YouTube without permission

13.1 RESPONDING TO INCIDENTS OF MISUSE

It is expected that all members of our Academy communities will be responsible users of digital technologies, who understand and follow policy. However there may be times when

infringements of the policy could take place, through careless or irresponsible or very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

1. The Network & MIS Manager in liaison with Head of School, Inclusion Manager and/or Executive Headteacher should be involved in the process and it will remain confidential. This is vital to protect individuals if accusations are subsequently reported.
2. The Network login will be disabled by Network &MIS Manager and the device will be quarantined where appropriate.
3. The procedure should be conducted using a designated computer that will not be used by anyone else and if necessary can be taken off site by the police should the need arise. The same computer should be used for the duration of the process.
4. Relevant staff will be able to access the Internet to conduct the procedure, and can draw down history from the Network or device if requested.
5. The URL of any site containing the alleged misuse and the nature of the content causing concern will be recorded.

In such cases it is important that all of the above steps are taken as they will provide an evidence trail. Once all the information has been gathered, a determination will be made whether there is a case to answer in line with our HR policies and procedures which may include referrals to external agencies including but not limited to the Police.

If the information gathered indicates a child has been harmed or is at risk of harm, monitoring and further investigation should be halted and referred to Local Authority Designated Officer (James McMillan Bexley LSCB) will be notified immediately as outlined in the Allegations Against Staff Policy.

14. RELATED DOCUMENTS, GUIDANCE & POLICIES

- Safeguarding Policy
- Behaviour Policy
- GDPR
- Staff Code of Conduct (Staff Handbook)
- Anti-Bullying Policy
- Risk Assessment Policy
- Teaching & Learning Policy
- Allegations Against Staff Policy
- PREVENT Policy
- E-Safety Acceptable User Agreements (Students & Staff)

****ESafety Policy will be updated annually in partnership with Governors, senior leadership team within each Academy and the Network & MIS Manager. However the Policy can and will be updated outside of this timeframe to reflect any changes in student/Academy need, local requirements and Government legislation.***

DOCUMENT REVISION

Date	Who	Description
April 2018	JB	Reviewed
Jun 2018	Governors	Approved