Kinsley Academy

E-Safeguarding Policy

December 2014

Why do we need an E-safeguarding policy?

Internet technologies and electronic communications provide children with exciting opportunities to broaden their learning experiences and develop creativity in and out of Academy. However, it is also important to consider the risks associated with the way these technologies can be used.

The E–Safeguarding Policy is in place to:

- Protect all staff and pupils.
- To set out the key principles expected of all members of the Academy community at Kinsley Primary, with respect to the use of ICT-based technologies.
- To assist Academy staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the Academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

This policy applies to the whole Academy community including the Academy board of governors, all staff employed directly or indirectly by the Academy and all pupils. The senior leadership team and Academy board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within Academy will be reflected within this policy.

At Kinsley Academy,

- Staff are aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct at all times is essential.
- All members of staff are aware that their online conduct out of Academy can have an impact on their role and reputation within Academy. Civil, legal or disciplinary action could be taken if staff members are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Any abuse or misuse of technology will be dealt with in line with the Academy behaviour policy.

Teaching and Learning

An eSafeguarding training programme will be established across the Academy to include a regular review of the eSafeguarding policy and pertinent points from the Academy eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within Academy. We will endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used. The eSafeguarding policy will be introduced to the pupils at the start of each Academy year and Safeguarding posters will be prominently displayed around the Academy

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the ICT curriculum / PSHE curriculum.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-Academy activities, including promoting Safer Internet Day each year.

- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline, cyber mentors or the CEOP report abuse button.

Staff training.

- Our staff receive regular information and training on eSafeguarding issues in the form of annual training and staff meetings when the need arises and to cascade information.
- As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the Academy's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the Academy community.
- All staff will be expected to incorporate eSafeguarding activities and awareness within their curriculum areas.

Internet Use

The purpose of Internet use at Kinsley Academy is to raise educational standards and to promote pupil achievement. Internet use is part of the statutory curriculum and is a necessary tool for learning. It is a part of everyday life for education and Academy has a duty to provide students with quality Internet access as part of their learning experience. Kinsley Academy allows Internet access to staff and pupils on the basis of educational need.

- All staff will read and sign the Academy Acceptable Use Policy before using any Academy ICT resources.
- Parents will be asked to read and sign the Academy Acceptable Use Policy for pupil access and discuss it with their child. This will be part of the home/Academy agreement. Pupils will be refused access to the internet until an AUP is received.

- All visitors to the Academy site who require access to the Academys network or internet access will be asked to read and sign an Acceptable Use Policy and will have limited access to the system, using a guest login.
- In Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration and then with directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools. Online activities will be teacher-directed where necessary.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, Academy management information system).
- Key Stage 1 pupils will have a generic 'pupil' logon to all Academy ICT equipment.
- Pupils at Key Stage 2 will have a unique, individually-named user account and password for access to ICT equipment and information systems available within Academy.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within Academy.
- Users are prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All access to Academy information assets will be controlled via username and password.
- No user should be able to access another user's files.
- Access to personal data is securely controlled in line with the Academy's personal data policy.
- The Academy maintains a log of all accesses by users and of their activities while using the system.

Internet Security and Filtering.

Kinsley Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Academy computer. Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children are always supervised when using the internet. In addition, Internet Safety Rules will be displayed in all areas where computers are located, both children and adults will be educated about the risks online. Any E-safeguarding incidents will be recorded on E-safeguarding log and this will be regularly monitored by the Senior Leadership Team.

Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

At Kinsley Academy,

- The Academy will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.

- The Academy uses a filtered internet service. The filtering system is provided by YHGFL and is appropriate to the age and maturity of pupils
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff will guide pupils to online activities that will support the learning outcomes and are appropriate for the pupils' age and ability
- The Academy will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- The use of Academy computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.

E-Safeguarding Incidents

E-Safeguarding risks can be experienced unintentionally or deliberately by people acting inappropriately. Any concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

An Incident Log to report breaches of filtering or inappropriate content being accessed is available in the ICT Suite and on the Teacher's shared drive. Any material that Academy believes is illegal must be reported to appropriate agencies such as IWF, Police or CEOP. Any illegal activity must be reported to the Designated Child Protection Coordinator.

- All members of the Academy community will be informed about the procedure for reporting E-Safeguarding concerns (such as breaches of filtering, cyber bullying, illegal content etc).
- The E-Safeguarding Coordinator will keep a record of all reported incidents and actions taken and this will be shared with the e-safeguarding committee.
- The Designated Child Protection Coordinator will be informed of any E-Safeguarding incidents involving Child Protection concerns, which will then be escalated appropriately.
- Academy will manage E-Safeguarding incidents in accordance with the Academy behaviour policy where appropriate.
- Academy will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the Academy will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Academy will contact the Children's Safeguard Team or E-Safeguarding officer and escalate the concern to the Police.
- Any complaint about staff misuse will be referred to the Head teacher.

Cyber bullying

Cyber bullying is "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone"

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other eSafeguarding-related incidents covered by this policy, which may take place out of Academy, but is linked to membership of the Academy.

At Kinsley Academy,

- Cyber bullying of any member of the Academy community will not be tolerated
- Clear procedures are in place to support anyone in the Academy community affected by cyber bullying. (see behaviour policy)
- All incidents of cyber bullying reported to the Academy will be recorded.
- Clear procedures are in place to investigate incidents or allegations of Cyber bullying.
- Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- We will take steps to identify the bully. This may include examining Academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the Academy to support the approach to cyber bullying and the Academy's E-Safeguarding ethos.

Sanctions for those involved in cyber bullying at Kinsley Academy,

- The bully will be asked to remove any material deemed to be inappropriate or a service provider will be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at Academy for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the Academys anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

E-Security & Data Protection.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

At Kinsley Academy:

- All access to personal or sensitive information owned by the Academy will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- Any access to personal and sensitive information, including Academy information management system should be assessed and granted by the SIRO (Paul Birdsall).
- All information on Academy servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff will not leave personal and sensitive printed documents on printers within public areas of the Academy.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.

- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the Academy's information-handling procedures and, for example, not left in cars or insecure locations.
- Personal data sent over the Internet or taken off site must be encrypted.
- Files held on the Academy's network are regularly checked.
- The use of user logins and complex passwords to access the Academy network will be enforced.
- Virus protection for the whole network is installed, current and updated regularly.

E-mail

E-mail is an essential means of communication for both staff and pupils. Email use can bring significant educational benefits but E-mail should not be considered private and Kinsley Academys reserve the right to monitor any email accounts accessed using Academy equipment. Pupil E-mail accounts should not be provided which can be used to identify both a student's full name and their Academy.

- Pupils may only use approved email accounts for Academy purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in emails, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used for communication outside of the Academy.
- Staff will only use official Academy provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team. Staff can not use personal email accounts for professional purposes.
- The forwarding of chain messages is not permitted.
- Pupils and staff will be made aware of the dangers of opening email or attachment from an unknown sender or source or viewing and opening attachments.
- The Academy requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the Academy'
- Academys will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

Social Networking and Blogs.

Social networking sites can connect people, users can be invited to view personal spaces and leave comments, over which there may be limited control. Children should be taught to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

Staff are aware of the potential risks of using social networking sites or personal publishing (blogs). Staff are fully aware of the importance of considering the material they post, they must ensure profiles are secured and understand how publishing unsuitable material may affect their professional status.

- Kinsley Academy will strictly control access to social media and social networking sites.
- Children will be taught never to give out personal details of any kind which may identify them and / or their location.
- Children will be taught about security and privacy online and they will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. They will be encouraged to approve and invite only known friends on social networking sites and to deny access to others by making profiles private.

- Concerns regarding children's use of social networking, social media and personal publishing sites (in or out of Academy) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain consent from the Head teacher before using Social Media tools in the classroom.
- Blogging, podcasting and other publishing of online content by pupils will take place within the Academy learning platform/YHGfL blog.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the Academy learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the Academy where possible.
- Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.
- Staff must ensure that any profiles on social media sites are set to maximum privacy.
- Staff must not accept 'friend' request from pupils or past pupils under the age of 18 on any personal social media websites.

Managing digital media – images and video conferencing.

Video conferencing enables users to see and hear each other between different locations. This 'real time' interactive technology and it has many uses in education.

At Kinsley Academy,

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing will be supervised appropriately for the pupils' age and ability
- Only key administrators are given access to video conferencing administration areas or remote control pages.
- Unique log on and password details for the educational video conferencing services are only issued to members of staff.
- Written permission from parents or carers will be obtained for use of photographs on the internet.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at Academy and at home.
- Pupils and staff will only use Academy equipment to create digital images, video and sound.
- Images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- Parents may take photographs at Academy events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites

- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the Academy network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils

The VLE

The VLE is subject to careful monitoring by the Senior Leadership Team. The SLT has a duty to annually review and update the policy regarding the use of the Learning Platform, and all users must be informed of any changes made.

- SLT will regularly monitor the usage of the VLE by pupils and staff.
- Pupils/staff will be advised about acceptable conduct and use when using the VLE.
- Only members of the current pupil, parent/carers and staff community will have access to the VLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff or pupils leave the Academy their account will be disabled or transferred to their new establishment.
- Any concerns about content on the VLE should be reported to the E-safeguarding co-ordinator or Head teacher.
- A visitor may be invited onto the VLE by a member of the SLT. In this instance there will be limited access.

Mobile phones and personal devices.

Mobile phones and other personal devices such as Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society. However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyber bullying;
- Internet access on phones and personal devices can allow pupils to bypass Academy security settings and filtering.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

For the reasons stated above any mobile phones or personal devices brought into Academy by pupils at Kinsley Academy will be taken to the main office, where they will be secured in a locked drawer. The pupil can have their device back at the end of the Academy day. Children needing to contact a parent during the Academy day can do so by speaking to a member of the office staff and using the Academy phone.

Staff and pupil at Kinsley Academy are aware that,

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden and any breaches will be dealt with as part of the Academy behaviour policy.

- Electronic devices of all kinds that are brought in to Academy are the responsibility of the user. The Academy accepts no responsibility for the loss, theft or damage of such items. Nor will the Academy accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Staff Use of Personal Devices.

- Staff are not permitted to use their own personal phones or devices for contacting children, parents or carers within or outside of the setting in a professional capacity.
- On trips a staff mobile is available to make contact with Academy/parents/carers.
- Mobile phones or devices will not be used during teaching periods unless permission has been given by the Head teacher in emergency circumstances.
- Staff must not use personal devices such as mobile phones or cameras to take photos or videos of pupils. Work-provided equipment must be used for this purpose.
- If a member of staff breaches the Academy policy then disciplinary action may be taken.

New Technologies

At Kinsley Academy we will keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies for use in the curriculum. Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment will be undertaken on each new technology to ensure effective and safe practice in classroom.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Academy Acceptable Use Policy.
- The Academy will periodically review which technologies are available within Academy for any security vulnerabilities that may have been discovered since deployment.
- All new technologies deployed within Academy will be documented within the eSafeguarding and Acceptable Use Policies prior to any use by any member of staff or pupil.
- Prior to deploying any new technologies within Academy, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.

Parental Support

Unless parents are aware of the dangers, children may have unrestricted and unsupervised access to the Internet in the home. Kinsley Academy will help parents plan appropriate, supervised use of the Internet at home and educate them about the risks.

- Parents' attention will be drawn to the Academy E–Safeguarding Policy in newsletters, the Academy prospectus, on the VLE and website.
- A partnership approach to E-Safeguarding at home and at Academy with parents will be encouraged.
- Parents will sign an E–Safeguarding/Internet agreement as part of the Home Academy Agreement.
- Information and guidance for parents on E–Safeguarding will be made available to parents in a variety of formats. VLE, Academy Website, workshops etc

Management of assets.

- Details of all Academy-owned hardware will be recorded in a hardware inventory.

- Details of all Academy-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The Academy will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Roles and Responsibilities.

The Senior Leadership Team.

- The headteacher is ultimately responsible for eSafeguarding provision for all members of the Academy community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator.
- The headteacher and senior leadership team are responsible for ensuring that the eSafeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

ESafeguarding Coordinator.

- To promote an awareness and commitment to eSafeguarding throughout the Academy
- To be the first point of contact in Academy on all eSafeguarding matters
- To take day-to-day responsibility for eSafeguarding within Academy and to have a leading role in establishing and reviewing the Academy eSafeguarding policies and procedures
- To communicate regularly with Academy technical staff
- To communicate regularly with the designated eSafeguarding governor
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that eSafeguarding education is embedded across the curriculum
- To ensure that eSafeguarding is promoted to parents and carers
- To monitor and report on eSafeguarding issues to the eSafeguarding group and the senior leadership team as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident

The eSafeguarding committee (SLT)

- To ensure that the Academy eSafeguarding policy is current and pertinent and reviewed on a regular basis.
- To ensure that Academy Acceptable Use Policies are appropriate for the intended audience

Teachers and support staff

- To read, understand and help promote the Academy's eSafeguarding policies and guidance
- To read, understand and adhere to the Academy staff Acceptable Use Policy
- To report any suspected misuse or problem to the eSafeguarding coordinator

- To develop and maintain an awareness of current eSafeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through Academy based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the Academy
- To maintain a professional level of conduct in personal use of technology at all times

Technical staff

- To support the Academy in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the Academy network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the Academy ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on Academy-owned devices
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to Academy-owned software assets is restricted

Pupils

- To read, understand and adhere to the Academy pupil Acceptable Use Policy
- To help and support the Academy in the creation of AUP's for pupils.
- To know and understand Academy policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in Academy and at home
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws
- To take responsibility for each other's safe and responsible use of technology in Academy and at home, including judging the risks posed by the personal technology owned and used outside Academy
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in Academy and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in Academy and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within Academy

- To discuss eSafeguarding issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the Academy in promoting eSafeguarding
- To read, understand and promote the Academy pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in Academy and at home
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the Academy if they have any concerns about their children's use of technology
- To agree to and sign the home-Academy agreement which clearly sets out the use of photographic and video images outside of Academy

Responsibilities of the governing body

- To read, understand, contribute to and help promote the Academy's eSafeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the Academy ICT infrastructure provides safe access to the internet
- To develop an overview of how the Academy encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of Academy
- To support the work of the eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of Academy, including encouraging parents to become engaged in eSafeguarding activities
- To ensure appropriate funding and resources are available for the Academy to implement its eSafeguarding strategy

Responsibilities of the Child Protection Officer

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose