This policy applies to the whole school including the Early Years Foundation Stage (EYFS)

The Policy is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office. All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours including activities away from school.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by the Headteacher and the Designated Safeguarding Leads (DSL), who will undertake a full annual review of this policy and procedures, including its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing. The Headteacher recognises that staff build expertise by undertaking safeguarding training and managing safeguarding concerns. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately. All staff will be informed of the update/reviewed policy and it is made available to them in either a hard copy or electronically.

Signed: *C.Redgrave* Date: September 2021

This policy was last reviewed by the Headteacher in September 2021 and will next be reviewed no later than **September 2022** or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Introduction: The primary purpose of this Policy is to safeguard pupils and staff at Eastcourt Independent School.

NOTE: Currently pupils at Eastcourt may not access the internet while on school premises. Any personal devices brought to school by pupils are handed in at the School Office at the beginning of the school day and returned at the end of school.

Therefore, E-safety policy at Eastcourt resolves itself, often via PSHEE, into advice about use and abuse of the internet and social media outside school. Instances of internet and social media abuse may be brought to Eastcourt's attention (or deduced from teacher-pupil interaction) after the fact, but the school accepts no responsibility for any individual pupil's use or abuse of the internet or social media outside school.

The policy details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole-school approach to e-safety. Our key message to keep pupils and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our E-Safety Policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding Children/Child Protection Policy (please refer to our Safeguarding Children/Child Protection Policy cited in related documents). Also see related documents to this E-safety Policy.

This policy informs and supports a number of other school policies, including our Safeguarding Children/Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. The staff and pupil Acceptable Use Policies (AUPs) are central to the E-safety Policy and should be consulted alongside this policy. The E-safety Policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. All staff should read these policies in

conjunction with the E-Safety Policy. This is particularly important with regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding Children-Child Protection and Preventing Extremism and Tackling Radicalisation Policies.

Roles and Responsibilities: Our nominated E-Safety Officer is Miss Hunswick who has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice and works closely with Mr Dart (our ICT teacher). This role overlaps with that of the DSL role and they work alongside the DSL in all matters regarding safeguarding and E-safety.

Their roles will include ensuring:

- Young people know how to use the internet responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- Pupils are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.
- To ensure that pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- All staff, volunteers and the proprietor receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- The Acceptable Use Policy (AUP) is to be implemented, monitored and reviewed regularly, all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be transparent and updated as agreed in school policies.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- That users may only access the networks and devices through a properly enforced password protection policy.

Staff/Volunteers Use of IT Systems:

Access to the internet and email is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT' (please see appendices) before using any school ICT resource. In addition:

- All staff will receive annual update e-safety training.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices. Staff are advised to follow the "How do I stay secure on the internet?" section in the E-Safety FAQ document.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study and monitor internet use closely. Every request to do so should be auditable with clear reasons for the need.
- The internet can be used actively to gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Additionally, staff should not communicate with pupils through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of lessons, activities or fieldtrips, must be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the school's E-Safety Officer.
2. The E-Safety Officer should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
5. No pupil or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read.

Teaching and Learning: Internet use is part of the curriculum and a necessary tool for learning. The internet is a part of everyday life for education, business and social interaction. Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security. E-safety is a focus in all areas of the curriculum and key e-safety messages are reinforced regularly, teaching pupils about the risks of internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour.

Staff should be vigilant in lessons where pupils use the internet. Staff will be provided with sufficient e-safety training to protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.

The school's internet access is designed to enhance and extend education. Pupils will be taught what internet use is acceptable and what is not and given clear guidelines. Access levels reflect the curriculum requirements and age of pupils. Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is a part of teaching/learning in every subject.

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- The school has a system for teaching internet skills in ICT lessons
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

Pupils Use of IT Systems: Pupils at Eastcourt Independent School will be given supervised access to our computing facilities and will be provided with access to filtered internet (see FAQ Document) and other services operating at the school. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of pupils and young people. The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law. Eastcourt Independent School will help pupils to understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also embedded in our Personal, Social, Health and Economic

Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- The UK Safer internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

Communicating and Educating Parents/Guardians in Online Safety: Eastcourt Independent School recognises the crucial role that parents play in the protection of their pupils with regards to online safety. The school organises an annual awareness session for parents with regards to e-safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents and carers with information through newsletters and web site. Parents and guardians are always welcome to discuss their concerns on e-safety with the school, who can direct them to the support of our E-Safety Officer/ICT teacher if required. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. The unauthorised access or use of personal information, contrary to the previsions of the Data Protection Act is not permitted. Virus protection will be updated regularly. If a 'virus alert' occurs when transferring work from one device to another a member of ICT staff should be informed immediately. All external hardware e.g. Memory sticks must be vetted by submitting them to an anti-virus check.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are not permitted to access their personal social media accounts using school equipment at any time
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media
- Pupils are not permitted to access their social media accounts whilst at school
- Staff and pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff and pupils are aware that their online behaviour should at all times be compatible with UK law.

Radicalisation and the Use of Social Media to Encourage Extremism: The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;
- Accessing likeminded people where they are not able to do this off-line, creating an online community;
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Eastcourt Independent School has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of E-Safety Issues and Concerns Including Concerns Regarding Radicalisation: Eastcourt Independent School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the E-safety Officer who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the e-safety officer. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children-Child Protection Policy.

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting pupils from the risk of on-line radicalisation. Eastcourt Independent School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of pupils and know where and how to refer pupils and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access.
- Emerging technologies, such as mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the E-Safety Policy is sufficiently robust and that the implementation of the E-Safety Policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The DSL will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *Wi-Fi* access.
- Eastcourt Independent School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking" (pg 33 Annex C of KCSIE 2021).
- Eastcourt Independent School recognises that pupils may choose to circumvent certain safety precautions by using devices over 3G and 4G. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/pupil training.

Internet Security and Filtering Systems

Eastcourt Independent School security has in place systems which monitor and secure the internet traffic at the school. These systems are to keep everyone safe, from blocking inappropriate content, to protecting our ICT systems from cyber-attacks. The monitoring side plays an important part of the system, which helps us to identify ways to improve security, and to better protect those that use it. By default, the system blocks all inappropriate websites, illegal or unsuitable content, including pornography. Use of these kinds of site is not allowed at the school.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; please see appendix 4 for more details).

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the e-Safety Officer, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Pupils of Eastcourt Independent School are only allowed to have mobile phones in school with advance permission from parents. Pupil mobile phones should be left with the office during the school day, and mobile phones which are kept on site are at the risk of the individual pupil. Eastcourt Independent School is not responsible for any devices lost by pupils.

Cyberbullying: is the use of ICT, particularly mobile electronic devices and the internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see our Safeguarding Children-Child Protection Policy).
Seven categories of cyberbullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to pupils or young people when they are in a web-based chat room;
- **Bullying through instant messaging (IM)** is an internet-based form of bullying where pupils and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, Google Hangouts etc.) as they conduct real-time conversations online;
- **Bullying via websites and social networks (an example of this would be Facebook, Twitter, Instagram, etc.)** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.

- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

ICT-Based Sexual Abuse: The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and storing indecent images of pupils is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils. Adults should ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Chat Room Grooming and Offline Abuse: Our staff needs to be continually alert to any suspicious activity involving computers and the internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents/carers are expected to sign a Home School agreement containing the following statement.
  We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute.
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
  - Posters
  - School website information

Taking and Storing Images of Pupils Including on Mobile Phones (See our related documents including Appendix 6): Eastcourt Independent School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in appendix 6 of this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published on any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy which includes:

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at Eastcourt Independent School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, visitors and parents/carers.
- How we inform parents/carers, visitors and other professional of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Computer Viruses

- All files downloaded from the internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If staff use a machine which is not routinely connected to the school network, they must make provision for regular virus updates through our IT team.
- If staff suspect there may be a virus on any school ICT equipment, they must stop using the equipment and contact ICT support immediately. The ICT support provider will advise staff what actions to take and be responsible for advising others that need to know.

Security

- The school gives relevant staff access to the network and specific files on the network
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Information Asset Owner (IAO): Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff should be able to identify across the school:

- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.
However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Email: The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsible online.

Managing email

- The school gives all staff their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school.' The responsibility for adding this disclaimer lies with the account holder
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
- Delete all emails of short-term value
- Organise email into folders and carry out frequent house-keeping on all folders and archives
- All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email
- Staff must inform (the e-safety co-ordinator) if they receive an offensive email
- Pupils are introduced to email as part of the Computing Programme of Study
- However, you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section
-
- Emailing Personal, Sensitive, Confidential or Classified **Information**
- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School email is not to be used for personal advertising

Receiving emails

- Check your email regularly
- Never open attachments from an untrusted source; consult your network manager first

Emailing Personal, Sensitive, Confidential or Classified Information: Where your conclusion is that email must be used to transmit such data:

Exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an email
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Please read in conjunction with 'internet Access Security' and EYFS ESafety – internet

Managing the internet

- The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- School internet access is controlled by the AVG Cloud software and regular checking.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from Headteacher, Deputy Head or ICT leader
- If there are any issues related to viruses or anti-virus software, Mr Dart and the Headteacher should be informed

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification

- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.

E-Safety FAQs

For more information relating to E-safety procedures, refer to the E-Safety Frequently Asked Questions (FAQ) in Appendix 5. It covers the following topics on the relevant page as follows:

1 How will the policy be introduced to pupils? How will staff be consulted and made aware of this policy? How will complaints regarding internet use be handled? How will parents' support be enlisted?
2 Why is the use of internet and ICT important? How is the safe use of ICT and the internet promoted? How does the internet and use of ICT benefit education in our school? How will pupils learn to evaluate internet content?
3 How is filtering managed? How are emerging technologies managed? How to react to misuse by pupils and young people
4 How is printing managed? What are the categories of Cyberbullying? What are the pupil rules?
5 What has research into Cyber Bullying found? What is the impact on a child of ICT based sexual abuse? What is the impact on a child of ICT-based sexual abuse? How do I stay secure on the internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy include?
6 Where can we learn more about Prevent? What do we have to do?
7 Do we have to have a separate *Prevent* Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
8 What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Related documents:

- E-Safety Appendices 1-6
- Safeguarding Children- Child Protection Policy; Anti-Bullying Policy; Behaviour and Discipline Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy, Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules.
- Taking and storing images of Pupils – Including Mobile Phones Policy; Acceptable use of ICT Sign off forms for Staff/Pupils; Use of Photographs Sign-off Form.
- What to do if you are worried; www.thinkyouknow.co.uk.

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Pupils Safe in Education* (KCSIE) *Information for all schools and colleges* (DfE: September 2021) incorporates the additional statutory guidance, *Disqualification under the Childcare Act 2006* (February 2015) and also refers to non-statutory advice for teachers, *What to do if you're worried a child is being abused* (HM Government: March 2015)
- *Working Together to Safeguard Pupils* (WT) (HM Government: 2015) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (March 2015) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (June 2015)* and *The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)*
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'

- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for school leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in schools.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; BECTA and CEOP.