Haberdashers'
Castle House School

A6xii Online Safety Policy

Actions	Date / details	By whom
Date originally published	March 2018	IS
Adopted by Governors	March 2018	Governors
Amendments	Aug 2025	IS
Adopted by Governors	Aug 2025	Governors
Review Date	Aug 2026 or before as required	

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 school's Designated Safeguarding Leads (DSL). The Governing Board will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing. The Governing Board 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 and without delay. All staff will be informed of the update/reviewed policy and it is made available to them in either a hard copy or electronically.

Introduction: The primary purpose of this Policy is to safeguard pupils and staff at Castle House School. It 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.

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 Online-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 Safeguarding Children – Child Protection 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 online-Safety Officer is the Headteacher who has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice. This role overlaps with that of the Designated Safeguarding Lead (DSL) role and he works alongside the DSLs 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 and volunteers 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, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- 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, in which passwords are regularly changed.

Pupils Use of IT Systems:

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, modelling 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 Childline.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via our teaching of ICT.

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 not allowed
- 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

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting E Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E Safety 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. The agreement will also include the following statement 'We will support the school's 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 into disrepute.
- 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).
- The school disseminates information to parents relating to E Safety where appropriate in the form of;
  - Posters
  - School website information
  - Awareness talks for parents with regards to Online Safety which looks at emerging technologies and the latest ways to safeguard pupils

Staff/Volunteers Use of IT Systems:

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

1. Report in confidence to the school's Online-Safety Officer.
2. The Online-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.

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, 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, pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, 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.

Castle House 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 online-Safety Issues and Concerns Including Concerns Regarding Radicalisation: Castle House 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. Castle House 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 Online-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 DSLs 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.
- Castle House 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" (KCSIE 2022).
- Castle House 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 provide relevant additional staff/pupil training.

Internet Security and Filtering Systems

Castle House 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. 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
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- 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 ICT support team, 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

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

No member of staff is allowed to use a personal mobile phone in the presence of pupils in the EYFS setting during the teaching day.

Castle House School Pupils are allowed laptops under the supervision of the SEN department. If a laptop is required, the pupil and parents will sign an agreement (see Appendix 8) that would allow the child to bring in their own device. Castle House School is not responsible for any damage or loss of the device. (Section 4.19 The Parent Contract). The laptop must be supplied with up to date antivirus software that is kept maintained weekly. The device will be subject to electrical testing when the school is tested yearly. The device must not be connected to the Castle House School network without the prior consent of the ICT Leader.

Cyber-Bullying: 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 cyber-bullying 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 cyber-bullying.

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.

Taking and Storing Images of Pupils Including Mobile Phones (See our related documents including Appendix 6): Castle House 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 onto 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 Castle House 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.

Computer Viruses

- All files downloaded from the Internet, received via e-mail 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): See appendix 7. 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 this member of staff 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.

E-mail: The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail 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 e-mail in relation to their age and how to behave responsible online.

Managing e-mail

- The school gives all staff their own e-mail 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 e-mails and avoids the risk of personal profile information being revealed
- The school disclaimer must be attached on any email that is sent from a school email address.
- 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 e-mail histories can be traced. The school email account should be the account that is used for all school business
- All e-mails 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
- E-mails 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 e-mail account as follows:
- Delete all e-mails of short-term value

- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil e-mail 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 e-mail 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 e-mail
- Staff must inform the E Safety and Head teacher if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of our teaching programme
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails
If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section

e-mailing Personal, Sensitive, Confidential or Classified Information: Where your conclusion is that e-mail must be used to transmit such data:
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail 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 e-mail is not to be used for personal advertising

Receiving e-mails
- Check your e-mail regularly
- Never open attachments from an untrusted source; Consult your network manager first

e-mailing Personal, Sensitive, Confidential or Classified Information: Where your conclusion is that e-mail must be used to transmit such data:

Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail 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)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

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 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 ICT leader
- If there are any issues related to viruses or anti-virus software, the Headteacher and the IT support provider should be in formed

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)
- 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 tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.

Online-Safety FAQs

For more information relating to online-safety procedures, refer to the online-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 Cyber-Bullying? What are the pupil rules for the ICT room?
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:

- Online-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 children Safe in Education* (KCSIE) *Information for all schools and colleges* (DfE: September 2022) 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: 2018) 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.

Policy Updated Sept 2022

Appendices

Appendix 1: EARLY YEARS FOUNDATION STAGE (EYFS) ONLINE-SAFETY, INTERNET AND ACCEPTABLE USE POLICY Updated August 2023

This policy, which applies to the whole school inclusive of the Early Years Foundation Stage, is in support of the health and safety policy and the individual health and safety assessments. This policy is publicly available on the school's website. On request a copy may be obtained from the school's office

Aim

The Acceptable Use Policy (AUP) will aim to:

- Safeguard pupils and young people by promoting appropriate and acceptable use of information and communication technology (ICT).
- Outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems.
- Ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Scope: The AUP will apply to all individuals who are to have access to and/or be users of work-related ICT systems. This will include pupils and young people, parents and carers, early years teachers and their coordinators, volunteers, pupils, committee members, visitors, contractors and community users. This list is not to be considered exhaustive. Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where known, off-site.

Roles and Responsibilities:

EYFS Coordinator: The ***EYFS Coordinator*** has overall responsibility for ensuring online safety and will be considered an integral part of everyday safeguarding practice. The EYFS Coordinator will liaise with the E-Safety Officer who will monitor the practice of e-safety within the EYFS. This will include ensuring:

- Early years teachers and their ***Coordinator*** will 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 AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be open and transparent.
- 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.

Designated Safeguarding Leads (DSLs): The Designated Safeguarding Lead (DSL)s have relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is to be available at all times.. The designated person for safeguarding will be responsible for ensuring:

- Agreed policies and procedures are to be implemented in practice.
- All updates, issues and concerns are to be communicated to all ICT users.
- The importance of online safety in relation to safeguarding is to be understood by all ICT users.
- The training, learning and development requirements of early years teachers and their coordinators are to be monitored and additional training needs identified and provided for.
- An appropriate level of authorization 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. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of pupils and young people will address online safety. A safe ICT learning environment is to be promoted and maintained.

Early years teachers and their co-ordinators: Early years teachers and their co-ordinators will ensure:

- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- ICT equipment is to be checked before use and all relevant security systems judged to be operational.
- Awareness will be raised of any new or potential issues, and any risks which could be encountered as a result.
- Pupils and young people are to be supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
- Online safety information is to be presented to pupils and young people as appropriate for their age and stage of development.
- Pupils and young people will know how to recognize and report a concern.
- All relevant policies and procedures are to be adhered to at all times and training undertaken as is to be required.

Pupils and young people: Pupils and young people will be encouraged to:

- Be active, independent and responsible learners.
- Abide by the Acceptable Use Agreement as to be approved by peers, early years teachers and their co-ordinators, parents and carers.
- Tell a familiar adult about any access of inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent).

Acceptable use by early years teachers and their co-ordinators:

Early years teachers and their co-ordinators should be enabled to use work-based online technologies:

- To access age appropriate resources for pupils and young people.
- For research and information purposes.
- For study support.

Use of images: displays etc.: We will only use images of our pupils for the following purposes:

- Internal displays (including clips of moving images) on digital and conventional notice boards within the school premises,
- Communications with the school community (parents, pupils, staff), for example newsletters.
- Marketing the school both digitally by website, by prospectus [which includes an iPad app], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

In the event of misuse by early years teachers or their co-ordinators: Should it be alleged, that an early years practitioner or manager is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report is to be made to the Headteacher or a Designated Safeguarding Lead immediately. Should the allegation be made against the Headteacher or Designated Safeguarding Lead, a report is to be made to the Chair of Governors. Procedures are to be followed as appropriate, in line with the ICT Misuse Procedure, Safeguarding Children-Child Protection Policy and/ or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

Acceptable use by pupils and young people: Pupils and young people will also be informed of the behaviours, which will be deemed unacceptable. This will allow pupils and young people to take some degree of responsibility for their own actions. Pupils will only be able to download a file under the direct supervision of a member of staff and it will be virus checked prior to being opened. The use of game-style activities and websites should be monitored by teachers to determine suitability.

Acceptable use by visitors, contractors and others: All individuals who affect or come into contact with the early years setting are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with pupils and young people. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.

Links to other policies

Behaviour Policy: The Behaviour Policy together with the anti-bullying contain up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyber-bullying. It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the 'real' and 'cyber' world and this is to be reflected in all relevant policies.

Safeguarding Children-Child Protection Policy and ICT Misuse Policy: The Safeguarding Children-Child Protection Policy and the ICT Misuse Policy are to be referred to when dealing with any incidents that should occur as a result of the intentional or unintentional misuse of ICT. Any allegations of abuse or other unlawful activity are to be reported immediately to the Designated Safeguarding Lead who will ensure procedures outlined in the Safeguarding Children-Child Protection Policy are followed with immediate effect.

Personal, Social, and Emotional Development: The promotion of online safety within PSED activities is to be considered essential for meeting the learning and development needs of pupils and young people. Key messages to keep pupils and young people safe are to be promoted and should be applied to both online and offline behaviours.

Health and Safety Policy: The safe use of ICT is included within the Health and Safety Policy, and should also include guidelines for the use of display screen equipment. The detrimental impact of prolonged ICT use on pupils' brain development should also be addressed.

Appendix 2 – PUPIL AND PARENT ACCEPTABLE USE POLICY Updated Aug 2023

Dear Parent

Online Safety Acceptable Use within School

ICT, including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E Safety rules overleaf with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the school either by calling: 01952 567600 or by email: admin@castlehouseschool.co.uk.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/children.

Kind regards,

Mr I Sterling
Headteacher

Primary School Pupil Acceptable Use
Online Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approves
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behavior when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher

E Safety - Acceptable Use within School. Parent Agreement

We have discussed this document with *(Insert Child's Name)* ……..... and we agree on their behalf to follow the E Safety rules and to support the safe use of ICT at Castle House School.

Full Name (Parent/Carer)

Signature …… Date……..

Appendix 3 - Acceptable Use of ICT Sign-off form for all staff at Castle House School: Aug 2023

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety Policy and ICT Acceptable Use Policy for further information and clarification. You must not use any ICT on-site until you have signed this Code of Conduct document and logged it with HR.

- I will respect all ICT equipment/facilities at Castle House School and will report any faults that I find or any damage that I accidentally cause.
- I agree to abide by this policy in respect of any of my own ICT equipment or mobile devices that I bring on site. If any ICT device (personal or school-issued) is being used inappropriately or illegally on site (or inappropriately in the presence of pupils), the Headteacher may request that the device be monitored. Failure to comply with the monitoring could result in informing the appropriate authorities.
- I understand that no photographs of pupils may be taken with or stored on my personal electronic devices, including cameras, iPads, mobile phones, or personal computers.
- Photos of pupils should not be uploaded to personal social media accounts
- I am familiar with the school's Data Protection Policy and I agree I am responsible for the security of all personal data in my possession. I agree that all personal data that relates to an identifiable person and is stored or carried by me on a removable memory device will be encrypted or contained within password-protected files to prevent unauthorised access.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others then I will immediately ask for these details to be changed.
- I agree that my use of Castle House School ICT equipment/facilities will be monitored and may be recorded at all times. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using Castle House School equipment/facilities. I understand that I may temporarily access-blocked websites, services and other online resources using only tools that are provided by Castle House School. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of Castle House School ICT equipment/facilities including the email and Internet system are for educational purposes, and personal use is not permitted provided
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on-site or using Castle House School equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not deliberately view, send, upload or download any material that is unsuitable for the school environment whilst I am in that environment or using any ICT equipment/facilities belonging to Castle House School. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the E-Safety Officer or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve e-safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the E-Safety Officer. I will not access any material that the E-Safety Officer has rated as unsuitable.
- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using Castle House School equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold Castle House School responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with pupils through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the school email system may be used.

Signed:_____ Date:_____

Appendix 4 *Mobile Phone Policy on the use of mobile technology, including taking and storing images of pupils* Updated Aug 2023

Legal Status:
This policy was prepared with reference to Ofsted advice on the use of mobile phones for the Early Years Foundation Stage (EYFS), the Department for Education's published guidance on the use of mobile phones and UK law governing the use of mobile phones while driving.

Applies to:
- The whole school including the Early Years Foundation Stage (EYFS), out of school care, the afterschool clubs, the holiday club and all other activities provided by the school, inclusive of those outside of the normal school hours.
- All staff (teaching and support staff), pupils on placement, the Headteacher, Governors and volunteers working in the school.

Related documents:
- ICT-Based Forms of Abuse (including Cyber-Bullying) Policy
- Safeguarding Children-Child Protection Policy
- Online-Safety Policy including ICT Acceptable Use

Availability:
This policy is made available to parents, staff and pupils via the School website and on request, a copy may be obtained from the Office.

Monitoring and Review:
- This policy will be subject to continuous monitoring, refinement and audit by the Principal.
- The Headteacher undertakes a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Introduction
Whilst we welcome the use of mobile phones and cameras for educational purposes and the convenience they offer and recognise that learning to use digital technology is an important part of the ICT and wider curriculum, equally we have to ensure the safeguarding needs of the pupils are met and staff, parents and volunteers are not distracted from their care of pupils. Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are associated risks. Pupils and young people must be encouraged to understand such risks, to enable them to develop the appropriate strategies which will keep them safe.

As with online safety issues generally, risks to pupils and young people should be broadly categorised under the headings of:
• Content
• Contact
• Conduct
• Commerce.

These issues are to be managed by reducing availability, restricting access and increasing resilience.
This philosophy is to be applied to the use of mobile phones through the Mobile Phone Policy. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses as to be agreed with the Designated Safeguarding Leads. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

Aims: The aim of the Mobile Phone Policy is to protect pupils and young people from harm, by ensuring the appropriate management and use of mobile phones by all individuals who work or visit our school. Pupils

and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use. This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Scope: The Mobile Phone Policy will apply to all individuals who are to have access to and or be users of personal and/ or work-related mobile phones within the broadest context of the setting environment. This will include pupils and young people, parents and carers, early years teachers and their co-ordinators, volunteers, pupils, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

Policy statement: It is to be recognised that it is the enhanced functions of many mobile phones that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and cyberbullying. It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to pupils and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Code of conduct: A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the pupils and young people in their care. It is to be ensured that all teachers and their co-ordinators will:

- Be aware of the need to protect pupils from harm.
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Be vigilant and alert to potential warning signs of misuse.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Be responsible for the self-moderation of their own behaviours.
- Be aware of the importance of reporting concerns immediately.

Guidance on Use of Mobile Phones by Teaching Staff Including those in the EYFS: The following points apply to all staff and volunteers at our school including those who teach in the Early Years Foundation Stage and apply to the use of all mobile devices to ensure the quality of supervision and care of the pupils, as well as the safeguarding of pupils, staff, parents and volunteers in the school.

Castle House School allows staff to bring in mobile phones for their own personal use. However, they must be kept locked away during ALL periods of contact time, and are not allowed to be used in the presence of pupils (this includes not using them on silent mode while pupils are in the classroom, i.e. during a test or quiz). They may be used during working hours in a designated break away from the pupils. Staff are not permitted to use recording equipment on their personal mobile phones to take photos or videos of pupils. If staff fail to follow this guidance, disciplinary action will be taken in accordance with Castle House School's Disciplinary Policy. During outings, nominated staff will be permitted to have access to their own mobile phones, which are to be used for emergency contact only. During off-site activities, i.e. field trips and overnight excursions, trip leaders will be provided with a school-issued mobile phone in good working condition. The sending of inappropriate text messages between any members of the school community is not allowed. Permission must be sought before any image or sound recordings are made on the devices of any member of the school community. Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used for school purposes. Where

the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Any other member of staff working within EYFS must ensure that they do not bring any other personal devices into classes. In the EYFS setting, school ICT (i.e. iPads. iPods and digital camera) will be used to evidence the pupils' personnel and learning development for the pupil. There are iPads with access to Wi-Fi owned by the school for the specific education purposes.

If staff need to make an emergency call, (such as summoning medical help or reporting an intruder on the premises) they must do so irrespective of where they are, via their own mobile phone or a school phone. Staff should provide the school number to members of the family and next of kin so in an emergency the member of staff can be contacted on the school phone.

There are film and digital cameras available for staff to use. Staff must ensure that there is no inappropriate or illegal content on their phones or mobile devices. Should any member of staff become aware of inappropriate or non-essential use of a mobile phone, this should be reported to a member of the Senior Leadership Team, and may be subject to disciplinary action.

Early Years Portfolios: Photographs taken for the purpose of recording a child or group of pupils participating in activities or celebrating their achievements is an effective form of recording their progression in the Early Years Foundation Stage and other areas of the school. However, it is essential that photographs are taken and stored appropriately to safeguard the pupils in our care. When pupils join our school we ask parents to sign consent for photographs and videos to be taken for such purposes.

All teachers are responsible for the storage of school cameras, which should be locked away securely when not in use. Images taken and stored on school cameras should be downloaded onto their school-issued computer and deleted from the cameras. Staff are not to use their own equipment to take photos of pupils. Under no circumstances must cameras of any kind be taken into the toilets (this includes any device with photographic or video capabilities). In the Early Years, photographs are sometimes distributed to members of key workers to record in pupils' profiles. Staff are not permitted to make extra copies of the photographs in any format.

Photographs are also taken at group events and activities and displayed around the child's room and in photograph albums for all the pupils to look back on and to talk about with their friends and teachers about the events that have happened in the EYFS. For this we need to have written parental permission for photo release that is requested upon enrolment. Every parent has the right to refuse this request, in which case the child must not be photographed by any member of staff, by a parent, or by any outsider without the express permission for that occasion of the parent with whom the EYFS has a contract.

Storage and Review of Images: Images of pupils are stored securely. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our web site, when expired material is deleted.

Castle House School Website and Facebook Page: Photographs and videos may only be uploaded to the school's website or Facebook (business page) with the Headteacher's approval. Pupil's surnames are never used on our website or Facebook page. When pupils join Castle House School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld such photographs/videos are not published of the individual child concerned. Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

External Photographers: Professional photographs are taken throughout the year at school shows, by local media and Professional School Portraits. The Principal ensures that professional photographers are DBS

checked and that they have their own stringent regulations, which ensure safeguarding of pupils from inappropriate use of images.

Appropriate use of a Mobile Phone during the School Day (Including Social Networking): Mobile phones have a place on outings or in school buildings, which do not have access to a school landline. In these cases, they are often the only means of contact available and can be helpful in ensuring pupils are kept safe. Ideally staff should use school mobile phones in these circumstances but, if required to use a personal phone, should input 141 to ensure their own number is hidden.

By arrangement with the Headteacher a member of staff's mobile phone may be designated as the means of communication for specific activities. The leader of the trip should ensure all participants (including parents, volunteers and partners) in the activity are aware of this Mobile Phone and Camera Policy.

When leaving the school building with pupils (e.g. for sport, or on school trips), the mobile phones of all members of staff must be switched on and turned to loud to ensure that staff can be contacted by the school. Contact numbers for all members of staff accompanying the pupils must be left at Reception and a list of contact telephone numbers for all pupils should be with the leader of the off-site activity (although these must be kept confidential). Group leaders will also be provided with a school-issued mobile phone.

Staff must not post anything onto social networking sites such as Facebook that could be construed to have any impact on the organisation's reputation. (We advise all our staff to carefully restrict their Facebook profiles to ensure they cannot be contacted by parents and pupils; this could involve removing their last name from their page). Staff must not accept friendship requests from parents or pupils at the school. Staff must not post anything onto social networking sites that would offend any other member of staff or parent using the setting. If any of the above points are found to be happening, then the member of staff involved will face disciplinary action, which could result in dismissal.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; please see appendix 4 for more details). Pupils at Castle House School are only allowed to have mobile phones in school with advance permission from parents, which is included in the parent acceptable use policy. This permission will be sought prior to the start of each school year. Pupils should ensure their mobile phones are left with the office at the start of school and collected at the end of the day. Mobile phones or other electronic devices which are kept on site, are at the risk of the individual pupil. Sinclair House School is not responsible for any personal devices lost or damaged whilst at the school.

Any use of mobile technology to intimidate, bully, harass, threaten or attempt to radicalise others or breach copyright laws will be counted as an infringement of network use and breach of discipline and will be dealt with in accordance with the school's policy for promoting positive behaviour. This may result in disconnection from the network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, School and statutory guidelines are not breached.

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.

The School has the right to confiscate and search any mobile electronic device (personal or school-issued) if it suspects that a pupil or staff member is in danger or has misused a device. This will be done in accordance with the School's policy on searching and confiscation as set out in the Behaviour and Discipline Policy.

Use of images: displays etc.
We will only use images of our pupils for the following purposes:

- Internal displays (including clips of moving images and yearbooks) on digital and conventional notice boards within School premises.
- Communications with Castle House School community (parents, pupils, staff), for example newsletters.
- Marketing Castle House School both digitally by website, by prospectus, by displays at educational fairs and other marketing functions and by other means.

Images that we use in displays and on our web site: The images that we use for displays and communications purposes never identify an individual pupil. Instead, they name the event, the term and year that the photograph was taken (for example, 'Sports Day, Summer Term 2016'). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a pupil. Pupils are always properly supervised when professional photographers visit Castle House School. Parents are given the opportunity to purchase copies of these photographs.

The pupils take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents present often take photographs of these memorable events, which may include groups of pupils. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents.

Media coverage: We will always aim to notify parents in advance when we expect the press to attend an event in which our pupils are participating, and will make every effort to ensure that images including pupils whose parents or guardians have refused permission for such images of their pupils to be used are not used. We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the pupils of celebrities.

Staff induction: All new teaching and office staff are given guidance on the school's policy on taking, using and storing images of pupils.

Use of Mobile Phones for Volunteers and Visitors: Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school. The exception to this would be at an organised event. Staff should remind parents regularly of school policy with regard to mobile phone use with the following statement on weekly emails, when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from the Data Protection Act 1998. Please be aware these images (which may include other pupils) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If they wish to make or take an emergency call they may use the office and the school phone.

Parental use of mobile phones/cameras within the school buildings: The growth of hand-held mobile technology and interconnectivity has implications for the safety of pupils, so in order to reflect the policy on safeguarding and child protection, it is essential parents do not use their mobile phones/cameras in the school building, apart from circumstances as outlined below. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of pupils or in public areas of the school such as during meetings and school events.

The school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

***Other mobile technology: At** Castle* House School*, we recognise the value of mobile technology within our curriculum. Any personal device that pupils bring to the school must be used appropriately in line with the Pupils' Acceptable Use Policy and must be kept securely. Where a pupil is found to be misusing a school*

or personal device, or accessing inappropriate content, the device may be confiscated by the school and appropriate action taken. When accessing the school Wi-Fi, staff and pupils must adhere to their ICT Acceptable Use Policy. Staff, pupils, volunteers and parents are responsible for their own mobile devices and the school is not responsible for theft, loss, or damage.

Driving and the law: The use of hand-held phones while driving, whether to make or receive a call, is prohibited. The only exception to this will be in the event of a genuine emergency call to 999 or 112, if it would be unsafe for the driver to stop. Hand-held mobile phones used with an earphone and microphone are covered under the ban, as they still require the user to hold the phone to press buttons or to read a message on the phone's screen.

The Headteacher of the school will not require any employee to receive or make calls on a mobile phone while driving. Mobile phones must instead be directed to the message/voicemail service while driving. Also, the Headteacher will not assist in the payment of any fine levied against anyone using a hand-held mobile phone while driving. An employee will be regarded as driving if the engine is running, even if the vehicle is stationery. Notification of any contravention of these requirements may be regarded as a disciplinary matter.

Appendix 5: *E-Safety FAQs*

How will the policy be introduced to Pupils?

- Rules for Internet access will be posted in all rooms where computers are used
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use will be included in the PSHE programme covering both home and school use.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Pupils will be made aware of the acceptable use of technology and sign upon enrolment

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers.
- Files held on the school network will be regularly checked
- All network system and administration passwords are to be recorded by the IT Department and kept in a secure place with regular updates

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Responsible Internet Use' statement included in the faculty handbook before using any Internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All staff including teachers, learning support assistants and support staff will be provided with the School e-Safety Policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read and sign *Staff Code of Conduct for ICT*- prior to using school ICT equipment in the school
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be dealt with by the Headteacher.
- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaint relating to the Headteacher must be referred to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children-Child Protection Policy and procedures.
- Pupils and parents will be informed of the complaint procedure.
- Parents and Pupils will need to work in partnership with staff to resolve issues.
- As with drug issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the responsible Internet use policy in newsletters and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- We will maintain a list of e-safety resources for parents.

- Parents will be invited to attend an e-safety workshop annually.

Why is the use of Internet and ICT important?
Not only is familiarity with the use of ICT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key – for example, the use of email for efficient communication and the correct use of the Internet for research. Staff across the school are making increased use of ICT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of ICT resources. In particular, ICT is extremely beneficial in engaging our pupils, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All pupils deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and Pupils. The school has a duty to provide Pupils with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (pupils and adults) everybody must be aware of the need to ensure on-line protection (e-safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the Safe Use of ICT and the Internet Promoted?
Castle House School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. Castle House School has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and Castle House School will further promote safe use of ICT and the Internet by educating pupils and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Pupils complies with copyright law. Castle House 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.
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)

How does the Internet and use of ICT benefit education in our school?
- Pupils learn effective ways to use ICT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between Pupils worldwide.
- Access to experts in many fields for Pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with Local Authority and DfE
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will Pupils learn to evaluate Internet content?
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- If staff or Pupils discover unsuitable sites, the URL (address) and content must be reported to the teacher, E-Safety Officer or IT Department.
- Staff and Pupils should ensure that their use of Internet derived materials complies with copyright law

- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed?

Having Internet access enables pupils to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to pupils. In addition, pupils' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our IT support team.. The IT support team will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of pupils. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at Castle House School we believe that the benefits to pupils having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of pupils along with Castle House School share the responsibility for setting and conveying the standards that pupils should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide pupils towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, they must report it to the ICT Coordinator immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect pupils from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are Emerging Technologies Managed?

ICT in the 21st Century has an all-encompassing role within the lives of pupils and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by pupils may include:

- The Internet
- E-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Social media
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / http://www.facebook.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com,http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'Internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

How to React to Misuse by Pupils and Young People

• **Step 1:** Should it be considered that a child or young person has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

• **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be

invited to discuss the incident in more detail with a senior administrator and the most appropriate course of action will be agreed.
• **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Children-Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is Printing Managed?
The use of the ICT printers may be monitored on an individual basis to encourage careful use of printing resources. As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with ICT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Pupils and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the printer and by using colour print only when necessary.

What are the categories of Cyber-Bullying? Seven categories of cyber-bullying 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.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to pupils or young people, or posting inappropriate material in a public digital locale.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** 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 cyber-bullying.

General Housekeeping:
The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes, but will consider doing so should the need arise.
The following will apply:
- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

What are the ICT Room Pupil Rules?
- Do not use ICT without permission.
- Food and drink must not be consumed near any computer equipment anywhere in the school.
- Do not move about the room while seated on a chair.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.

- Computer faults should be promptly reported to the ICT Co-ordinator. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.
- At the end of a session:
- Log off/shut down according to instructions.
- Replace laptops as directed.
- Wind up and put away any headsets.

What has Research into Cyber Bullying Found?

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by pupils in the same class or year group and although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

- Between a fifth and a quarter of pupils have been cyber-bullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyber-bullying.
- There is more cyber-bullying outside school than in.
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyber-bullied tell no one about the bullying.

What is the impact on a child of 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.

How do I stay secure on the Internet?

- Do not type any personal details (including your name or email address) into a web site unless you are absolutely sure of the authenticity and trustworthiness of the associated company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the principal.

Why is Promoting Safe Use of ICT Important?

Sinclair House School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

What does the school's Mobile Phone Policy Include?

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at Castle House 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.

Prevent – Top ten FAQs
We are receiving a number of queries to the support@isi.net inbox concerning inspection expectations in relation to the *Prevent* strategy so it may be useful if we address the most frequently asked issues.

1. Where can we learn more about *Prevent*?
There are two key source documents for the *Prevent* strategy:
 statutory guidance (Home Office) – see paras 1-27 generally and 57-76 for sector specific guidance for schools

 Advice for schools (Department for Education)

2. What do we have to do?
The over-arching legal duty is to **"have due regard to the need to prevent people from being drawn into terrorism"** and, in so doing, have regard to guidance issued by the Secretary of State. In summary, the national statutory guidance from the Home Office, and sector-specific advice from the Department for Education places the following expectations on schools:

 Demonstrate effective leadership: display an awareness and understanding of the risk of radicalisation in your area and institution; communicate and promote the importance of the *Prevent* duty to staff; ensure staff implement the *Prevent* duty effectively.

Train staff: ensure staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism; 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 and are shared by terrorist groups; ensure staff know where and how to refer pupils and young people for further help.

Work in partnership with other agencies: co-operate productively, in particular, with local *Prevent* co-ordinators, the police and local authorities, and existing multi-agency forums, for example Community Safety Partnerships; ensure that safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children's Board (LSCB).

Share information appropriately: ensure information is shared between organisations to ensure, for example, that people at risk of radicalisation receive appropriate support.

Risk assess: assess the risk of pupils being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This should be based on an understanding, shared with partners, of the potential risk in the local area or your school's particular circumstances. This means being able to demonstrate both a general understanding of the risks affecting pupils and young people in the area and a specific understanding of how to identify pupils who may be at risk and what to do to support them.

Build resilience to radicalisation: promote fundamental British values through the curriculum and through social, moral, spiritual and cultural education; equip pupils with knowledge, skills and understanding to prepare them to play a full and active part in society; ensure your school is a safe place to discuss sensitive issues, while securing balanced presentation of views and avoiding political indoctrination.

Safeguard and promote the welfare of pupils: put in place robust safeguarding policies to identify pupils at risk, and intervene as appropriate by making referrals as necessary to Channel or Children's Social Care, for example.

Ensure suitability of visiting speakers: operate clear protocols for ensuring that any visiting speakers, whether invited by staff or by pupils themselves, are suitable and appropriately supervised.

IT policies: ensure pupils are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to the ICT curriculum and can also be embedded in PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups. It is for schools to use their own judgement to fill in operational detail about how best to implement the duty in the context of the level of risk in their locality as advised by their Local Safeguarding Children Board (LSCB) or other local agencies and the assessed risks to their own pupils. The role of inspectors is to raise awareness of the duty and consider whether the measures schools have in place appear effective in each school's particular context. In particular, inspectors will check that schools know how to respond to pupils who may be targeted or influenced to participate in radicalism or terrorism.

Do we have to have a separate *Prevent* policy?
The Prevent duties can largely be implemented through schools' existing safeguarding duties using, for example, current reporting lines and training processes. It is not a requirement to create a separate dedicated *Prevent* Policy. However, the Home Office statutory guidance introduces a new requirement that policies "set out clear protocols for ensuring that any visiting speakers – whether invited by staff or by pupils themselves – are suitable and appropriately supervised." This protocol can be a standalone document or be part of another policy or document.

What IT filtering systems must we have?
No technical guidance has been prescribed concerning the levels of filtering which are to be considered appropriate. This means that schools have discretion as to how they approach this aspect of the prevent duty. Inspectors will assess and challenge on the basis of whether what is in place appears effective in practice to ensure pupils are kept safe from terrorist and extremist material when accessing the Internet in school. Keeping safe on-line is as much about educating pupils to think critically and about appropriate behaviour on-line as technical solutions.

What is the definition of a visiting speaker?
There is no definition of a visiting speaker. Schools should exercise their own reasonable judgement to determine who is a visiting speaker.

Do we have to check all our visiting speakers?
Schools must ensure all visiting speakers are suitable. There is scope for local discretion as to how. For example, a school could choose to check all speakers or to check all those whom risk assessment indicates warrant closer attention. The over-arching strategy should be recorded in the written protocol mentioned above.
When it comes to inspection, the burden is on the school to demonstrate to inspectors how they meet the duty. Inspectors will expect verbal assurances from schools to be backed up by documentary and other evidence that protocols are put into practice on the ground.

What checks must we run on visiting speakers?
The means by which schools ensure the suitability of their speakers are not prescribed (except in the event that they happen to come within any of the usual categories in the Independent School Standards and Keeping Children Safe in Education, such as "staff"). Schools need not confine their approach to the usual formal checks; Internet searches, for example, may sometimes be more instructive than formal vetting checks.
This is compatible with KCSIE which advocates in para. 43 that "... governing bodies and proprietors should prevent people who pose a risk of harm from working with pupils by adhering to statutory responsibilities to check staff who work with pupils, taking proportionate decisions on whether to ask for any checks beyond what is required; and ensuring volunteers are appropriately supervised". © Independent Schools Inspectorate 2015.

What do we have to record in our Single Central Register about visiting speakers?
The formal recording requirement for the SCR have not changed. Schools must decide which, if any, formal checks are required and must be recorded in the SCR by reference to the usual considerations such as role, frequency, supervision, payment (as not all visiting speakers are volunteers), whether speakers are employed by another organisation.
What training must we have?
As a minimum, schools should ensure that the Designated Safeguarding Lead/s undertakes Prevent awareness training and are able to provide advice and support to other members of staff on protecting pupils from the risk of radicalisation. Schools should consider and arrange further training in the light of their assessment of risks.

What are the potential legal consequences if we do not take the *Prevent* duty seriously?
Where the Secretary of State is satisfied that a school has failed to discharge the duty under the Prevent strategy to have regard to the need to prevent people from being drawn into terrorism, the Secretary of State may give directions to the school to enforce performance of the duty. A direction can be enforced by court order.

What are the rules for publishing content online?

- Staff or Pupil personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Pupil's full names will not be used anywhere on the school website or other on-line space.
- We may use photographs of pupils or their work when communicating with parents and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of pupils in swimwear would be inappropriate).

Appendix 6 – Parents, volunteers and visitors photographing pupils. Updated Aug 2025

Castle House School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. The growth of hand-held mobile technology and interconnectivity has implications for the safety of pupils, so in order to reflect the policy on safeguarding and child protection, 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 below. This includes where pupils are on school trips or residential. Neither are volunteers or visitors are permitted to take photographs or recordings of the pupils. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of pupils. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school.

Parental use of mobile phones/cameras whilst on the school grounds
Castle House School allows parents to take photos of their own children at organised events such as a school performance, sporting event or celebration of learning. We will remind audiences of this at the start of each event, where practicable. Staff will also remind parents regularly of school policy with regard to mobile phone use with the following statement when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from the Data Protection Act 1998. Please be aware these images (which may include other pupils) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If parents wish to make or take an emergency call whilst on school grounds, they may use the office and the school phone.

Parents are welcome to take photographs of their own pupils taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply. Additionally, the school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

When pupils join Castle House School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The pupils take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of pupils. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of pupils who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of the Data Protection Act 1998 without consent of all people within the photograph.

USE OF PHOTOGRAPHS OF PUPILS AND DATA PROTECTION FORM (To be completed by all new parents)

Photographs

Castle House School would like your permission to use photographs of your child for marketing and publicity purposes including our website, prospectus, adverts, press releases and other marketing literature such as brochures and leaflets. We will not use names next to photographs of pupils on the website (in accordance with the DfE guidelines). This form is in addition to Castle House School's standard terms and conditions which states "Parents' consent to Castle House School making use of information (textual or pictorial) relating to their child whilst they are at Castle House School and after they have left for the purpose of marketing and publicity for the school."

Parent/Carer's name: _____

Pupil's name: _____

Pupil's year group/form: _____

Please tick the appropriate box.

I give my permission for Castle House School to use photographs of my child for marketing and publicity purposes ☐

I do not give my permission for Castle House School to use photographs of my child for marketing and publicity purposes ☐

Signature: _____ Date: _____

Data Protection Statement

In addition to paragraph Castle House School's standard terms and conditions relating to the use of data about you and your child, information about parents is collated, stored and used by Castle House School for the purposes of keeping you informed of events and activities concerning Castle House School and for fundraising. By signing this form, you consent to Castle House School using your data in this way. This information will not be used for any other purpose or passed to any person outside the school without your consent.

I consent to Castle House School using my data for the stated purposes ☐

I do not consent to Castle House School using my data for the stated purposes ☐

Signature: _____ Date: _____

Appendix 7 - Illegal Incidents Reporting

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.