



Online Safety Policy 2025/2026

Date Approved	September 2025
Signed by Chair of Governors	
Renewal Period	Annual

INTRODUCTION

This policy document sets out the school's aims, principles and strategies for the delivery of Information and Communication Technology ensuring the online safety of system users.

This policy considers all current and relevant issues, in a whole school context, linking with other relevant policies and agreements, such as the ICT Acceptable Use Agreement, Child Protection and Health & Safety policies.

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers & visitors) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

STATEMENT of INTENT

Broughton Jewish understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, self-harm and suicide, discriminatory or extremist views, misinformation, disinformation (including fake news), and conspiracy theories as recognised online safeguarding harms.

Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

LEGAL FRAMEWORK

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2025) Keeping children safe in education
- DfE (2025) Working together to improve school attendance
- DfE (2023) Teaching online safety in school
- DfE (2023) Plan technology for your school
- DfE (2024) Generative AI: product safety expectations
- DfE (2018) Searching, screening and confiscation

- National Cyber Security Centre (2017) Cyber Security: Small Business Guide
- UK Council for Child Internet Safety (2020) Education for a Connected World – 2020 edition
- UK Council for Child Internet Safety (2017) Sexting in schools and colleges: Responding to incidents and safeguarding young people
- DfE (2021) Harmful online challenges and online hoaxes

THE SCHOOL'S AIMS

The ability to use ICT effectively is an essential life skill in our modern society. Our aim is to produce learners who are confident and effective users of ICT who develop skills that are transferable to all subject areas.

Pupils interact with the internet and other communications technologies such as mobile/smart phones and other forms of mobile devices on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction is greatly beneficial but can occasionally place young people in danger.

Online safety comprises all aspects relating to children and young people and their safe use of the internet, mobile phones and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of our 'Duty of Care'.

This policy highlights our responsibility to educate children and young people about the benefits, risks and responsibilities, of using information and communication technologies and provides safeguards and awareness for uses to enable them to control their online and wireless experiences.

The internet is an open communications channel, available to all. Applications such as e-mail, blogs and social networking all transmit information over the internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with very little restriction. These features of the internet make it an invaluable resource used by millions of people every day. Much of the material on the internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime, racism, etc that would be more restricted elsewhere. Pupils must also be made aware of the possible consequences of the imputing of their own data and other information. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online

safety policy is used in conjunction with other relevant school policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build our pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

SCOPE OF THE POLICY

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Where a member of staff misuses the school system this may lead to disciplinary action being taken.

ROLE AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for ICT development and online safety of individuals and groups within the school:

The Governors will be responsible for ensuring that:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

The Academy Principal

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis
- The Academy Principal and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

The DSL will be responsible for:

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians and the Online Safety Officer.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Works closely with the Online Safety Officer to ensure a whole-school, uniform approach.

The Online Safety Officer will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns ensuring that the DSL is kept informed of any concerns.
- Monitoring online safety incidents, using Securly, to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Working with the academy principal and governing body to update this policy on an annual basis.
- day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety procedures
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.

The School Business Manager will be responsible for:

- medium and long term hardware planning ensuring curriculum needs are met
- managing the budget for ICT and the provision of resources and consumables
- ensuring the operational effectiveness of the ICT Network and any managed service provider.
- ensuring that resources are maintained and repaired as needed

The School Business should also ensure that any Technical Support should cover the schools infrastructure and ensure:

- Servers, wireless systems and cabling are securely located and physical access is restricted
- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the online safety technical requirements outlined in any school Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the online Safety Co-ordinator for investigation / action / sanction.

- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- They make their Line Manager and the Business Manager aware of curriculum developments that may require updates to computer hardware or software.
- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Online Safety Officer for investigation/action/sanction
- Digital communications with parents / pupils (email / voice) should be on a professional level and only carried out using official school systems. **Staff should never use personal email or phone numbers to contact parents.**
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Senior Lead for child protection

should be trained in online safety issues and be aware of the potential for serious child Protection issues to arise from:

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

Pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (depending on age).
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy.

MONITORING AND FILTERING

Broughton Jewish Cassel Fox Primary School uses Securly for monitoring and filtering the content which our staff and pupils access when using online devices. The DSL and Online Safety Officer will record incidents involving staff and children on CPOMS and take appropriate action where necessary.

In addition:

- The school will use the DfE's Plan technology for your school service to review filtering and monitoring provision and ensure compliance with national expectations.
- The school will ensure filtering and monitoring includes the safe use of generative AI, in line with the DfE's Generative AI: product safety expectations.
- The school will adopt recognised cyber security standards to strengthen technical safeguarding measures and resilience against cyber threats.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Broughton Jewish Cassel Fox Primary School recognises that AI has many uses, including enhancing teaching and learning.

However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. In the interest of safeguarding, Broughton Jewish Cassel Fox Primary School will treat any use of AI to access harmful content or bully pupils in line with this policy and our behaviour and anti bullying policy. This can be found on the school website.

In regards to staff use of AI, all staff **have been made aware** of the risks of using AI tools whilst they are still being developed and should carry out risk assessments for any new AI tool being used by the school, consulting with the computing lead if they have any concerns. Any use of AI to improve teacher workload will be conducted through the lens of our GDPR policy and no identifying factors will be used.

As the use of AI in the educational sector evolves, this policy will be updated.

ONLINE SAFETY EDUCATION AND TRAINING

The curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationship and Health Education
- PSHE
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

The online risks pupils may face online are always considered when developing the curriculum. The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and CFC. Relevant members of staff, e.g. the SENCO and designated teacher for CFC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with pages 15 to 18 of this policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the school's reporting procedure.

Training and Support for pupils

Online safety education will be provided in the following ways:

- A planned online safety programme will be provided as part of Computing lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key online safety messages will be reinforced as part of a planned programme of IT activities
- Pupils will be taught in all lessons where IT is in use to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

Training and Support for Staff

- A regular audit of staff IT skills will be undertaken, identifying areas for development and training needs. All staff will be given the opportunity to attend courses to update their skills as required. Training will be made available for all staff in school, including non-teaching staff. ICT specialist teachers are encouraged to keep their skills up to date with time provided for attendance at suitable training events, where appropriate.
- We believe that all staff should have access to ICT equipment for their own professional use and have provided computers in the staff room and laptops assigned to individual members of staff for use at home.

Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Website updates with useful sites and information
- Where possible, external training delivered by a reputable organisation

Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Links to the school's information management system (CPOMS)

- The schools administration database holds confidential data about the pupils; staff access to information held on the system will be appropriate to their role with school. Access to parent contact information is restricted by access rights on the system.

HEALTH AND SAFETY

- The school has a Health and Safety Policy, which is available to all staff. Staff, where appropriate and so far as is reasonably practicable, are responsible for their health and the pupils they supervise.

RESPONSIBLE USE

- Pupils and parents/carers are made aware of the Rules for Responsible Use which forms part of the schools online safety arrangements. This is issued annually and updated as appropriate. All pupils and parents/carers sign to show their agreement to the school rules. Staff are required to sign a Staff Acceptable Use Agreement.

TERMINOLOGY

The school is committed to using language in line with the SEND Code of Practice (2015).

Outdated terms such as “spectrum disorder” are avoided and inclusive, up-to-date terminology is used throughout policies and practice.

SECURITY OF SYSTEMS

Physical Security

The risks associated with having a large number of computers in school have been assessed. All computers are asset tagged with details held within the schools inventory system.

Data Security

- all staff and students using network computers must save data to network drives where backups are carried out daily
- when working on lap-tops, or other computers not connected to the internet, data must be stored to an external encrypted drive.
- Staff must never store personal data relating to staff or pupils onto a lap-top computer
- Staff must never store pupils work that forms part of their external examinations on a staff lap-top, such work should never be taken off-site
- Staff must at all times comply with the data protection act and General Data Protection Regulations; further advice can be obtained from the online safety officer and/or Data Protection Officer.
- On-site data servers are locked securely at all times with back-ups taken daily which are stored off-site via Computeam.
- all original discs are held securely

In addition staff must not leave data or confidential information on systems to which pupils have access.

Virus protection

Staff are made aware of the issues surrounding the spread of virus infection and the following steps taken:

- all administration and curriculum machines in school are installed with virus protection software which is regularly updated
- software brought into school will not be installed onto computers unless its origin is known and the correct licence is available. Software must only be installed by the IT support
- all staff and pupils will be made aware of the risks of virus infection from work carried on external data drives

- all staff and pupils are made aware of the risks from virus infection from attachments to email and these will be virus checked before they are opened

Remote learning

All remote learning is delivered in line with the school's Pupil Remote Learning Policy.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

Pupils not using devices or software as intended will be disciplined in line with the Behavioural Policy.

The school will assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will consult with parents at least two weeks prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

COMMUNICATION DEVICES AND METHODS

The following table shows the school's policy on the use of communication devices and methods. Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

Communication method or device	Staff & other adults				Students/Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
								
Mobile phones may be brought to school (pupils must hand in devices on arrival to the school office)								
Use of personal mobile phones in work time								
Use of school owned mobile phones in work time								
Use of mobile phones in social time								
Taking photos on personal mobile phones or other personal camera devices								

Use of personal hand held devices eg iPads								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of chat rooms / facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								



This table indicates when some of the methods or devices above may be allowed:

Circumstances when these may be allowed		
Communication method or device	Staff & other adults	Students/Pupils
Use of school owned mobile phones in work time	School purchased phones are issued to the Principal, Headteacher and DSL and may be used for work related purposes	
Use of mobile phones in social time	Mobile phones may be used during unpaid breaks (lunch) within staff social areas, eg, lunchtime. Staff <u>must not</u> give their personal contact details to pupils/parents.	
Use of personal email addresses in school, or on school network	Staff may access personal e-mails during unpaid breaks (lunch). Personal e-mails <u>must never</u> be used to communicate with pupils/parents.	
Use of instant messaging	Staff may send personal instant messages during periods of unpaid breaks (lunch). Personal messaging systems <u>must never</u> be used to communicate with pupils/parents.	
Use of social networking sites	Only allowed by staff employed to maintain communication systems eg Twitter accounts	

Use of blogs	To communicate with pupils/parents for school related purposes.	
--------------	---	--

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use **only** the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the online safety officer– in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. **Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.**
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school. In addition the school policy restricts certain internet usage.

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions					
child sexual abuse images					
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					
adult material that potentially breaches the Obscene Publications Act in the UK					

criminally racist material in UK					
Pornography					
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					
promotion of racial or religious hatred					
threatening behaviour, including promotion of physical violence or mental harm					
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					
Using school systems to run a private business					
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					
Creating or propagating computer viruses or other harmful files					
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					
online gaming (educational)					
online gaming (non educational)					
online gambling					
online shopping / commerce					
Use of social networking sites					
Use of video broadcasting eg Youtube					
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)					

INCIDENTS

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If any apparent or actual misuse appears to involve illegal activity, these are incidents that must be reported directly to the police. This will be done through the school's Designated Safeguarding Lead.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials, e.g. Incidents of 'grooming behaviour', the sending of obscene materials to a child.

In the event of the above occurrence CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.

They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

All adults should know who the Designated School Lead for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such an event, more than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

INCIDENT MANAGEMENT

Incidents - Pupils:	Refer to class teacher	Refer to online Safety Officer or DSL	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		☒	☒	☒		☒			
Unauthorised use of non-educational sites during lessons	☒	☒				☒			
Unauthorised use of mobile phone/digital camera / other handheld device	☒	☒				☒			
Unauthorised use of social networking/ instant messaging/personal email		☒	☒			☒			
Unauthorised downloading or uploading of files		☒				☒			
Allowing others to access school network by sharing username and passwords	☒	☒				☒			
Attempting to access or accessing the school network, using another student's/pupil's account	☒	☒							
Attempting to access or accessing the school network, using the account of a member of staff		☒	☒			☒			
Corrupting or destroying the data of other users		☒				☒			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		☒	☒			☒			

Continued infringements of the above, following previous warnings or sanctions						☒	☒	☒	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			☒			☒		☒	
Using proxy sites or other means to subvert the school's filtering system		☒				☒			
Accidentally accessing offensive or pornographic material and failing to report the incident		☒				☒			
Deliberately accessing or trying to access offensive or pornography		☒	☒			☒		☒	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		☒							

Incidents - staff:	Refer to line manager	Refer to Headteacher/online safety officer	Refer to HR Advisor	Refer to Police	Refer to technical support company for action re filtering / security etc	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		☒	☒	☒				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		☒						

Unauthorised downloading or uploading of files		☒						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		☒	☒					☒
Careless use of personal data eg holding or transferring data in an insecure manner	☒	☒	☒					
Deliberate actions to breach data protection or network security rules	☒	☒						☒
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	☒	☒				☒		☒
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☒	☒	☒			☒		☒
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	☒	☒	☒			☒	☒	☒
Actions which could compromise the staff member's professional standing		☒	☒			☒	☒	☒
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		☒				☒	☒	☒
Using proxy sites or other means to subvert the school's filtering system	☒	☒			☒			
Accidentally accessing offensive or pornographic material and failing to report the incident		☒	☒			☒	☒	☒
Deliberately accessing or trying to access offensive or pornographic material		☒	☒			☒	☒	☒
Breaching copyright or licensing regulations	☒	☒				☒		
Continued infringements of the above, following previous warnings or sanctions							☒	☒

STAFF GUIDANCE

Social Networking Sites and other forms of Social Media.

Employees who choose to make use of social networking sites/social media should ensure

- That they familiarise themselves with the sites 'privacy setting' in order to ensure that information is not automatically shared with a wider audience than intended.
- That they do not conduct or portray themselves in a manner which may;-
 - bring the school into disrepute;
 - lead to valid parental complaints;
 - be deemed as derogatory towards the school and/or its employees;
 - be deemed as derogatory towards pupils and/or parents and carers;
 - bring into question their appropriateness to work with children and young people.
- That they do not form online 'friendships' or enter into communication with parents/carers and students as this could lead to professional relationships being compromised.
- They do not engage in online friendships and communications with former students under the age of 18.

Further information and guidance

Further information on online safety for adults and young people can be obtained from the Child Exploitation and online Protection Centre (CEOP): www.ceop.police.uk