On-line Safety Policy
2019/20

Date Approved	7.11.19
Signed by Chair of Governors	D Black
Committee Delegated	Leadership, Management & Quality of Education
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 on-line 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.

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 transferrable to all subject areas.

Pupils interact with the internet and other communications technologies such as mobile/smart phones and other forms of mobile device 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.

On-line 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
- Unauthorized 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 on-line 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 on-line 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 on-line 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 on-line safety of individuals and groups within the school:

The Academy Principal and Governors will be responsible for ensuring that:
- ICT development is incorporated into the academies long term plans to ensure the necessary resources are available to meet curriculum needs
- there is appropriate technical support for ICT
- appropriate teaching support is available
- training needs are assessed regularly and opportunities for staff to receive the necessary training are made available
- a monitoring process of the delivery of ICT in the school is in place
- the performance of the schools IT provision is monitored
- there is an overview of on-line safety (as part of the wider remit of Child Protection) across the school.
- 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 on-line safety allegation being made against a member of staff

On-line Safety Officer will be responsible for:
- day to day responsibility for on-line safety issues and has a leading role in establishing and reviewing the school on-line safety procedures
- ensuring that all staff are aware of the procedures that need to be followed in the event of an on-line safety incident taking place.
- provides training and advice for staff
- receives reports of on-line safety incidents and creates a log of incidents to inform future on-line safety developments.
- liaison with school based IT staff and any managed service provider.
- reports regularly to Headteacher and Senior Leadership Team

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 on-line 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 On-Line 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 on-line safety matters and of the current school on-line 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 On-Line 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.**
- on-line safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school on-line 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 on-line 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 on-line 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 on-line 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 on-line safety campaigns/literature. Parents and carers will be responsible for:

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

ON-LINE SAFETY EDUCATION AND TRAINING

Training and Support for pupils

On-line safety education will be provided in the following ways:

- A planned on-line safety programme will be provided as part of ICT lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key on-line 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 on-line 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.

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

- 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 on-line 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.

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 on-line safety officer and/or Data Protection Officer.
- the school 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

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

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

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.

	Staff & other adults				Students/Pupils			
Communication method or device	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 camera devices				☒				☒
Use of personal hand held devices eg iPods				☒				☒
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 must not 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 must never 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 must never 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 on-line 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				☒	
On-line gaming (educational)				☒	
On-line gaming (non educational)				☒	
On-line gambling				☒	
On-line 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 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 On-line Safety Officer or DSI	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/on-line 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 on-line 'friendships' or enter into communication with parents/carers and students as this could lead to professional relationships being compromised.
- They do not engage in on-line friendships and communications with former students under the age of 18.

Further information and guidance

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