

Ref: Online Safety Policy  
Approved by Governors: November 2020  
Reviewer: Business Manager/November 2021

## ONLINE SAFETY/ICT POLICY



### Governing Body Approval

Policy approved by:

\_\_\_\_\_  
(NAME)  
  
\_\_\_\_\_  
(SIGNATURE)  
  
\_\_\_\_\_  
(GOVERNOR POSITION)  
  
\_\_\_\_\_  
(DATE)

## **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 IT Acceptable Use Agreement, Child Protection and Health & Safety policies.

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

## **THE SCHOOL'S AIMS**

The ability to use IT effectively is an essential life skill in our modern society. Our aim is to produce learners who are confident and effective users of IT 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 users 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 inputting 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 students' 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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. 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 IT development and on-line safety of individuals and groups within the school:

#### **The Headteacher and Governors will be responsible for ensuring that:**

- IT development is incorporated into the School Development Plan to ensure the necessary resources are available to meet curriculum needs
- there is appropriate technical support for IT
- 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 IT 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 Headteacher 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 IT and the provision of resources and consumables
- ensuring the operational effectiveness of the IT Network Staff and any managed service provider.

**Network Manager:**

is responsible for ensuring:

- ensuring that resources are maintained and repaired as needed
- ensuring servers, wireless systems and cabling are securely located and physical access is restricted
- That the school's IT 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 relevant Local Authority On-Line Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are changed regularly
- 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 / Virtual Learning Environment (VLE) / 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
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

**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 students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- 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 IT 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 Person 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 IT 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.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the schools Online Safety Policy covers their actions out of school, if related to their membership of the school

### **Parents/Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local on-line safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school IT systems or Learning Platform in accordance with the school 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 IT lessons and will be regularly revisited – this will cover both the use of IT and new technologies in and outside school
- Key on-line safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils will be taught in all lessons 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**

- An 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. IT specialist teachers are encouraged to keep their skills up to date with time provided for attendance at suitable training events, where appropriate. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff will be made aware of the On-line Safety Policy and school requirements.
- We believe that all staff should have access to IT equipment for their own professional use and have provided computers in the staff room and laptops and iPads assigned to individual members of staff for use at home.
- This Online Safety Policy and its updates will be discussed by the Online Safety Officer in staff training days.

### **Links to the school's information management system (SIMS)**

- 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.

### **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 IT Acceptable Use Policy. This is incorporated in the Personal Planner and updated annually as necessary. 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**

#### **Infrastructure**

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (as advised by external service provider)
- There will be regular reviews and audits of the safety and security of school technical systems and the Network Manager is responsible for acting on advice given
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password periodically.
- The “master / administrator” passwords for the school IT system, used by the Network Manager must also be available to the Headteacher and School Business Manager and kept in a school safe
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. All filtering changes must be approved by the Online Safety Officer
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for different ages / stages and different groups of users such as staff / pupils
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems must be approved by the School Business Manager.
- All executable programmes must be installed by the Network Management team
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **Physical Security**

The risks associated with having a large number of computers in school have been assessed and the following steps have been taken to ensure the security of the systems;

- all computers are asset tagged with details held within the schools inventory system
- the school/computer rooms are alarmed with police response activated on the second activation of the burglar alarm

### **Data Security**

- all staff and students using network computers must save data to network drives where backups are carried out daily
- staff are responsible for ensuring their device is locked when not in use (Ctrl+Alt+Delete – Lock This Computer)
- when working on lap-tops, or other computers not connected to the internet, staff should save data to the school network by Remote Access. Where this is not possible data must be stored to an encrypted external drive, such as a USB Pen Drive, a second copy of this data should be kept. Data must never be stored to the hard-drive of a lap-top computer or other mobile device.
- 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 General Data Protection Regulations, further advice can be obtained from the Business Manager
- the school on-site data servers are locked securely at all times with back-ups taken daily which are stored separately
- data stored to network drives is held securely, backup copies are saved to the Spirit of Sport.
- all original discs are stored separately in a locked cabinet

In addition, staff will 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
- care is taken when installing programs, from any source, to ensure they are clear of virus infection and only installed by the school network staff
- software brought into school will not be installed onto computers unless its origin is known and the correct licence is available
- all staff and students will be made aware of the risks of virus infection from work carried on external data drives
- all staff and students are made aware of the risks from virus infection from attachments to email and these will be virus checked before they are opened
- if virus infection is suspected action will be taken at once to ensure protection of the system

## Mobile Technologies (including BYOD/BYOT)

- Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
- All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, Use of Social Networking Sites Policy apply at all times.































## 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.

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	iPad	Student owned	Staff owned	Visitor owned
Allowed in school	✓	✓	✓	✓	✓	✓
Full network access	✓	✓	✓		✓	
Internet only				✓	✓	
No network access						✓



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								
Use of mobile phones in lessons								
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, PDAs, PSPs								
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:

Communication method or device	Circumstances when these may be allowed	
	Staff & other adults	Students/Pupils
Use of mobile phones in lessons	To demonstrate/lead lessons using mobile technology for items such as QR readers.	Under the direction of a classroom teacher when used to support learning
Use of mobile phones in social time	Mobile phones may be used during unpaid breaks, eg, lunchtime. Staff must not give their personal contact details to pupils/parents.	
Use of personal hand held devices eg PDAs, PSPs	To demonstrate/lead lessons using device functionality, eg, video recording within subject teaching.	Under the direction of a classroom teacher when used to support learning
Use of personal email addresses in school, or on school network	Staff may access personal e-mails during unpaid breaks. Personal e-mails should not be used to communicate with pupils/parents.	
Use of social networking sites	To communicate with pupils/parents using the schools twitter account for school related purposes. Staff should not access social networking sites of pupils.	
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 and VLE may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service and/or VLE to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – 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, VLE 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 when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<b>User Actions</b>					
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					
File sharing					
Use of social networking sites					
Use of video broadcasting eg Youtube					
Accessing the internet for personal or social use (e.g. online shopping)					
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 IT, 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, i.e.

- 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.

These are incidents that must be reported directly to the police. This will be done through the school's designated Child Protection officer.

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 Person 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 Head of Department/on-line safety officer	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)		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			
Unauthorised use of non-educational sites during lessons	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Unauthorised use of mobile phone/digital camera / other handheld device	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Unauthorised use of social networking/ instant messaging/personal email		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			
Unauthorised downloading or uploading of files		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Allowing others to access school network by sharing username and passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Attempting to access or accessing the school network, using another student's/pupil's account	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							
Attempting to access or accessing the school network, using the account of a member of staff		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			
Corrupting or destroying the data of other users		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			
Continued infringements of the above, following previous warnings or sanctions						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Using proxy sites or other means to subvert the school's filtering system		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Accidentally accessing offensive or pornographic material and failing to report the incident		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Deliberately accessing or trying to access offensive or pornography		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		<input checked="" type="checkbox"/>							

<b>Incidents - staff:</b>	Refer to line manager	Refer to Headteacher/on-line safety officer	Refer to Local Authority /HR	Refer to Police	Refer to technical support staff 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)		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		<input checked="" type="checkbox"/>						
Unauthorised downloading or uploading of files		<input checked="" type="checkbox"/>						
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		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		
Careless use of personal data eg holding or transferring data in an insecure manner	<input checked="" type="checkbox"/>							
Deliberate actions to breach data protection or network security rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

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 college into disrepute;
  - lead to valid parental complaints;
  - be deemed as derogatory towards the college 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):

## **Appendix 1 – Staff & Volunteer, Acceptable Use Agreement**

### **Staff and Volunteer Acceptable Use Agreement**

To ensure that all adults within the school setting are aware of their responsibilities when using any IT equipment and communications, such as the internet or e-mail, they are asked to sign this Acceptable Use Agreement. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies and protect themselves so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.



#### **For my professional and personal safety:**

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed on-line safety in my work with young people.

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email, VLE etc) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the on-line safety officer.

#### **Rules for Staff**

##### **I will be professional in my communications and actions when using school IT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school, or using school equipment, in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will ensure that I follow the Data Protection Act 1998 and understand that it is my responsibility to know what this involves.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Senior Person for Child Protection or on-line safety Leader.
- I know who the Designated Person for Child Protection is.



**I will work with the school and the local authority to provide safe and secure access to technologies and ensure the smooth running of the school:**

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school on-line safety policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**I will access materials on the internet in my professional capacity or for school sanctioned personal use in an appropriate manner:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**I understand that I am responsible for my actions in and out of school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read; understood and agree with the above rules and know by following them I have a better understanding of on-line safety and my responsibilities to safeguard children and young people when using on-line technologies. I understand that it is my responsibility to read and understand the schools On-Line Safety Policy and other associated policies such as Child Protection.

Staff / Volunteer Name

--

Signed

--

Date

--

<b>Designated Senior Person For Child Protection</b>	Jo McCue	<b>On-Line Safety Leader</b>	Dionne Swift / Elizabeth Fleming
--	----------	------------------------------	--