Balby Carr Community Academy
ICT Acceptable Use Policy 2017

Policy last update: Jan 2017 / next review date: Jan 2018

ICT and Internet use at Balby Carr Community Academy

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

The purpose of ICT use in the college is to raise educational standards, to promote pupil achievement, to support professional work of staff and to enhance the schools management, information and business administration systems.

The internet is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The college has a duty to provide students with a quality Internet access as part of their learning experience. While the college has put in place internet filtering and security systems to help safeguard students they have full access to the Internet outside college so need to learn how to evaluate Internet information and to take care of their own safety and security.

How the Internet Benefits Education

The Internet provides access to worldwide educational resources including museums and art galleries; educational and cultural exchanges between pupils worldwide; vocational, social and leisure use in libraries, clubs and at home; access to experts in many fields for pupils and staff; access to learning wherever and whenever convenient .

The Internet also promotes professional development for staff through access to national developments, educational materials and good curriculum practice. Teachers can share lesson plans and resources with colleagues and other schools around the world using resources like Learning Platforms and ePortals.

The Internet also provides improved technical support including remote management of networks and automatic system updates.

Enhanced Learning through the use of the ICT and Internet

Fast reliable Internet access in the college is provided by Virgin Media and is filtered using Smoothwall web filter managed by the college ICT Support Team.

Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research and taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

ICT System Security

The school ICT systems are protected by Windows 2008 Server group policies with tiered levels of restrictions to ensure users have the appropriate access level. All computers are actively monitored by Securus to detect any security, cyberbullying and other safeguarding concerns. All computers are protected with Sophos Antivirus which automatically updates on a daily basis. Users must only use their user account to access the college computers and ensure they secure the computer when they leave it as they are responsible for all activity on their user account.

Any data sent over the Internet or taken off site, including on laptop, must first be encrypted, instructions on how to encrypt files are in the appendix. The use of mobile media such as USB memory drives is discouraged as they are a security risk that can transmit viruses, can easily be damaged or lost. Only the ICT Support Team should install software on the college computer systems and any unapproved programs, system utilities and files will be deleted from the network to ensure ICT System Security.

Email

Email is an essential means of communication and all staff are provided with a work email account to communicate with parents/carers, pupils and other professionals for any official school business. Pupils may only use approved email accounts for school purposes and must immediately tell a designated member of staff if they receive offensive email. Pupils must not reveal personal details of themselves or others in communication, or arrange to meet anyone without specific permission from an adult.

Excessive social email use can interfere with learning and will be restricted. The forwarding of chain letters and junk email is not permitted. Staff should not use personal email accounts during working hours or for professional purposes.

College Website

The college website provides various points of contact including the college address, telephone number, fax number and email address. Staff and pupils' personal information must not be published. Email addresses will be published carefully online, to avoid being harvested for spam by replacing the '@' with 'AT'. The head teacher will take overall responsibility for online content published by the college and will ensure that the content published is accurate and appropriate. The college website will comply with the college's guidelines for publications including respect for intellectual property rights, privacy policies and copyright. The copyright for all material published must be held by the school, or attributed to the owner where permission to reproduce has been obtained.

Use of Student Photographs

Still and moving images and sound add liveliness and interest to a publication, particularly when students can be included. Nevertheless the security of staff and students is paramount. Although common in newspapers, the publishing of students' names with their images is not acceptable. Published images could be reused, particularly if large images of individual students are shown.

Strategies including using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or a team activity. Students in photographs should be appropriately clothed.

Images of a pupil must not be published without a parent's or carer's written permission. Pupils also need to be taught the reasons for caution in publishing personal information and images online.

Social Networking, Social Media and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking can connect people with similar or even very different interest. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms, instant messenger and many others.

The school will control access to social media and social networking sites like Facebook and Twitter. Pupils will be advised never to give out personal details of any kind which may identify them and /or their location. Examples would include real name, address, mobile or landline numbers, school name, IM and email addresses, full names of friends/family, specific interest and clubs etc.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis. Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Internet Filtering and Website Access Control

The college has a dedicated Internet Filtering and Web Access Control server from Smoothwall that has dynamic content analysis to accurately categorise and block undesirable content. Website signature scanning prevents the use of anonymous proxies. Active Directory integration allows user accounts to be linked to activity allowing full monitoring and reports to be generated to investigate user access. A second security server from Securus logs key strokes for all text and analyses patters for inappropriate content capturing screens to allow reports to be produced.

Internet filtering covers all devices on the college network but staff should be mindful that with modern technology students may gain access to unfiltered Internet using their own mobile devices such as phones and tablets so staff should make sure that students are supervised and aware of the Acceptable Use Policies in place. In addition, the Responsible ICT Use poster should be displayed, a copy of which is attached to this policy.

Websites which users believe should be blocked should be reported to the ICT Support Team. Teachers should always evaluate any websites / search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc just before the lesson. Remember that a site considered safe one day may be changed doe to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time a web page is accessed.

New Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. Emerging technologies will

be examined for educational benefit and a risk assessment will be carried out before use in the college is allowed. Pupils will be instructed about safe and appropriate use of personal devices both on and off site.

Personal Data and the Data Protection Act 1998

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

All staff computers and laptops have access to SIMS and Staff Common, these contain personal details of both staff and students and therefore under no circumstances must students be allowed to use these computers. All computers are password protected and staff should not leave their computer unattended when they are logged in, if you are leaving the room either lock the computer by holding the Windows Start Menu key down and pressing L or log off the computer completely.

Staff should ensure that students cannot inadvertently view data on the screen or projected image on the whiteboard including from outside the room through a window.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorised Internet Access

Before any user is allowed to access the Internet they must sign to say they have read the Acceptable Use Policy. Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate. All visitor to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy. Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability. When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable

material will never occur via a school computer. Neither the school nor Doncaster MBC can accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to South Yorkshire Police. Methods to identify, assess and minimise risks will be reviewed regularly.

Complaints Procedure

Any complaint about misuse, such as breaches of filtering, cyberbullying, illegal content etc, should be referred to the IT Manager who will take the appropriate action. Any complaints about staff misuse will be referred to the head teacher. The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or
- A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

ePortal Learning Platform

An effective learning platform offers a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It enables pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

SLT and staff will regularly monitor the usage of the ePortal by pupils and staff in all areas, in particular message and communication tools and publishing facilities. Pupils/staff will be advised about acceptable conduct and use when using the LP. Only members of the current pupil, parent/carers and staff community will have access

to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the ePortal. When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

Any concerns about content on the LP may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.

A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot. Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Mobile Phones and Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA , MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

Due to the widespread use of personal devices it is essential that mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy. School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Mobile phones and personal devices will not be used during lessons or formal school time unless students are instructed to do so by staff for use in relation to teaching and learning requirements. They should be switched off at all times. The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones. Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Staff will be issued with a school phone where contact with pupils or parents/carers is required. Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. If a member of staff breaches the school policy then disciplinary action may be taken.

Legal Framework

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud);
- or impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image”
63 (6) must be “grossly offensive, disgusting or otherwise obscene”
63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/antibullying policy.

eSafety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Cybermentors: www.cybermentors.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Acknowledgements

This policy has been written by Lee Elvin, building on the eSafety Policy Template provided by Kent County Council and government guidance.

ICT Acceptable Use Policy 2015

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, iPads, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Support Team.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the ICT Policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school ICT Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection and e-Safety Coordinator Jane Shaw as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Jane Shaw the e-Safety Coordinator or Lee Elvin the designated lead for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Team as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator Jane Shaw or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.