Allenton Community Primary School

We care that our children understand, believe in, and achieve their full potential.

eSafety and Data Security

Policy for ICT Acceptable Use

Revision: 1.1
Date: 23/06/16
Author(s): SLT

Document Control			
Version	**Date**	**Author**	**Description**
1	5/06/15	J.Fordham	
2	23/06/16	SLT	

Document Review Schedule			
Review Date	**Committee**	**Committee Chair**	**Completed Review Date**

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At ACPS**,** we understand the responsibility to educate our pupils on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors[for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by that provider.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. For staff any policy breach is grounds for disciplinary action in accordance with the school's Disciplinary Procedure. For pupils, reference will be made to the school's behaviour policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or Safeguarding Team. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

eSafety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns. The school will maintain the following information:-

Allenton Community Primary School eSafety Incident Log

Details of ALL eSafety incidents will be recorded by the Safeguarding team. This incident log will be monitored weekly by the Headteacher. Any incidents involving Cyberbullying will be recorded in the Headteacher's Incident File also.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

Complaints

Complaints and/or issues relating to eSafety should be made to the Safeguarding team or Headteacher. All incidents should be logged.

Inappropriate Material

- All users must familiarise themselves with the procedures for reporting accidental access to inappropriate materials. (See Appendix 1 and 2). The breach must be immediately reported to the Headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Acceptable Use Agreement: Pupils

See Appendix 1

Acceptable Use Agreement: Staff, Governors and Visitors

See Appendix 2

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and report it to the school ICT Co-ordinator immediately. The ICT Co-ordinator will advise you what actions to take and be responsible for advising others that need to know.

Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This includes a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
- The school will maintain a comprehensive inventory of all its ICT equipment on its school audit inventory, including a record of disposal. The disposal record will include the date the item is disposed of and its authorisation for disposal.

E-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing e-mail

The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external parents are advised to cc. the Headteacher.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You should therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform their Team Leader if they receive an offensive e-mail
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your line manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of the school community have been made aware of who holds this post. It is the role of the ICT Co-ordinator to keep abreast of current issues and guidance through organisations such as Derby City LA, CEOP (Child Exploitation and Online Protection) and Childnet

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Anti-Bullying, Safeguarding and Home–School agreements.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing/ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see Headteacher).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet

and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and parent workshops.

The Internet

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Particular consideration must be given to any references to the school or anyone connected with the school bearing in mind the wide audience of any communication. Social networking, e.g. Facebook, Twitter and Instagram and texting is a way of life for many adults. Staff and Governors should be aware of the potential risk to their professional reputation and that comments made on a social network site which relate to the school, pupils, staff or governors could lead to a disciplinary action. Please observe the following:

- Staff and Governors should not use school equipment, or the school internet connection, to access or update personal social websites.
- Staff and Governors should not have any child under 18 as "friends".
- It is strongly recommend that Staff and Governors do not have parents or ex-pupils as "friends."
- Staff and Governors should use strong passwords and apply security settings so that all aspects of their profile are secure and controlled; this includes linked social networks such as Twitter feeds or Instagram being duplicated on Facebook pages.
- Staff and Governors should NOT post anything, on a social website or text, about the school community including about incidents, pupils, staff or governors.
- Staff and Governors are expected to uphold professionalism and dignity on a public website, which would include the use of language, including profile name, and content, including photos. They should think of this in respect of being a role model. Staff and governors should not use inappropriate comments in relation to gender, race, disability, age, religion or sexual orientation.
- Staff and Governors should ensure that any views given on social networking sites are clearly stated, in a disclaimer, as their own personal views and not those of the school.
- Images of pupils taken during school time or on educational visits must **never** be posted.
- Images of work colleagues or governors should not be posted without their permission. Alternatively online albums may be made that are only accessible to those who are in the photographs.
- Professional use of networks such as PLN (Professional Learning Network) can be used to develop a useful and interesting professional dialogue, contributing to staff CPD.

Infrastucture

School internet access is controlled through the school's Websense web filtering service which is the responsibility of the school's network manager. Filtering is actively monitored at all times.

ACPS is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Headteacher.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored
- At present, the school endeavors to deny access to social networking and online games websites to pupils
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents must not take photographs or videos of events that occur during school activities, unless given specific authorization from the school to do so.
- Any images, videos or information from school activities taken by parents, when authorized by the school, must only be for personal use and not shared or posted online.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Intake evenings
    - Practical training sessions e.g. current eSafety issues
    - Posters
    - School website information
    - Newsletter items

Passwords and Password Security

Passwords

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform the Headteacher immediately**

If you think your password may have been compromised or someone else has become aware of your password report this to your line manager

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, learning platform and Management Information System log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen (hold down the windows key and press the L key once) before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you copy, scan or print.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site and Twitter
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. Pupils' full names will not be published. Before posting pupil work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images/ films of children are stored on the school's network

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- Deleting the images when they are no longer required, or when the pupil has left the school is the responsibility of the ICT Co-ordinator.

Webcams

- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions.
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- The school uses ischoolaudit to record all ICT equipment issued to staff and records serial numbers as part of its asset management.
- Visitors should not plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your line manager. You must also provide details of all your system logons so that they can be disabled
  All ICT equipment allocated to staff must be authorised by the ICT Co-ordinator. The ICT Co-ordinator is responsible for:

    - maintaining control of the allocation
    - recovering and returning equipment when no longer needed

Portable & Mobile ICT Equipment

This covers such items as laptops, mobile devices and removable data storage devices.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. Staff are not permitted to use their mobile phones during normal working time.
- Pupils are not routinely allowed to bring personal mobile devices/phones to school. If it is deemed essential, parents must complete a disclaimer form and the phone must be handed in to the school office for safekeeping. At all times the device must be switched onto silent
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

1.1.1 School Provided Mobile Devices (including ipads)

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Servers

- Servers are kept in a locked and secure environment
- Access rights are limited
- The server is password protected and locked
- Existing servers have security software installed appropriate to the machine's specification
- Backup hardware is encrypted by appropriate software
- Data is backed up regularly
- Backup discs are securely stored in a fireproof container
- Backup media stored off-site is secure
- Remote backups are automatically securely encrypted.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Twitter to communicate with parents and carers.
- Staff ***are not*** permitted to access their personal social media accounts using school equipment at ***any time during school hours***
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Telephone Services

School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.

School Policy in Brief

- At this school we have an Acceptable Use policy which all staff sign. Copies are kept on file.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.
  Protect and Restricted material must be encrypted if the material is to be removed from the school.
- At this school we use automatically encrypted flash drives for this purpose and limit such data removal.
- At this school we use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using Office 365 and/or egress switch.

Sensitive or personal material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in filing cabinets in either the school office, Headteacher's office or Learning Mentor/SENCO's room.
- At this school all servers are in a lockable location with a key-pad entry system in place and managed by DBS checked staff.
- At this school we follow LA back-up procedures.

Disposal: Sensitive or personal material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use a recommended disposal firm for the disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedure.
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, Frog (Learning Platform) access are limited to senior staff.
- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.

Appendix 1

Pupil Acceptable Use Agreement

eSafety Rules

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

Dear Parent/Carer,

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

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school.

It is also important that parents confirm that they will comply with the school policy regarding parents taking or sharing images, videos and information about school events, as outlined in page 8 of the eSafety policy as follows:

- Parents must not take photographs or videos of events that occur during school activities, unless given specific authorization from the school to do so.
- Any images, videos or information from school activities taken by parents, when authorized by the school, must only be for personal use and not shared or posted online.

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

Parent/Carer Signature

We have discussed this document with _____(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Allenton Community Primary School.

We also agree to follow the eSafety rules for parents regarding the taking and sharing of images, videos or information about school activities.

Parent/Carer Signature _____
Class _____ Date _____

Appendix 2

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature _____ Date _____

Full Name _____ (printed) Job title _____