Airedale Infant School
Ambition · Bravery · Respect

E-Safeguarding Policy
September 2020

E-safety relates to many parts of the curriculum, including ICT, citizenship and PHSE. 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 children with the skills to access life-long learning and employment.

Internet access is an important learning tool for schools. Access to the internet and a wide range of resources for learning is considered essential and plays a major role in any learner's development.

At Airedale Infant School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is who has been designated this role as a member of the senior Management team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such Wakefield LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head/e-Safety coordinator updates Senior Management and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety policy

The schools e-safety policy is part of the schools safeguarding policy and is by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and is updated regularly in accordance with the evolution of digital technologies.

Policy introduction

- To set out the key principles expected of all members of the school community at School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Scope of policy

- This policy applies to the whole school community including Schools Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

- AIS Schools' senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.

- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or 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 cyberbullying, or other e-Safeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-Safeguarding behaviour that takes place out of school.

Review and ownership

- The school has appointed an e-Safeguarding coordinator who will be responsible for document ownership, review and updates.
- The e-Safeguarding policy has been written by the school e-Safeguarding coordinator and is current and appropriate for its intended audience and purpose.

- The school e-Safeguarding policy has been agreed by the senior leadership team and approved by governors.

- The e-Safeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

- The School has appointed a member of the governing body to take lead responsibility for e-Safeguarding.

- All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

Communication policy

- AIS schools' senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school e-Safeguarding policy and the use of any new technology within school.

- The e-Safeguarding policy will be provided to and discussed with all members of staff formally.

- All amendments will be published and copies will be able to Governors and Staff.

- An e-Safety unit will be included in the PSHE and ICT curricula covering and detailing amendments to the e-Safeguarding policy.

- An e-Safeguarding or e-Safety training programme will be established across the school to include a regular review of the e-Safeguarding policy.

- e-Safeguarding or e-Safety training will be part of the transition programme across EYFS and KS1 and when moving between establishments, pupils' responsibilities regarding the school e-Safeguarding policy will be reviewed.

- The school council will act as an integral part to the deliverance of safety to the pupil body.

- Pertinent points from the school e-Safeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.

- The key messages contained within the e-Safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.

- We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used

- The e-Safeguarding policy will be introduced to the pupils at the start of each school year

- E-Safeguarding posters will be prominently displayed around the school to highlight the importance of staying safe in today's evolving digitally rich society.

Roles and responsibilities

We believe that e-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute

Responsibilities of the senior leadership team

- The headteacher is ultimately responsible for e-Safeguarding provision (including e-Safeguarding) for all members of the school community, though the day-to-day responsibility for e-Safeguarding will be delegated to the e-Safeguarding coordinator.

- The headteacher and senior leadership team are responsible for ensuring that the e-Safeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their e-Safeguarding roles and to train other colleagues when necessary.

- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal e-Safeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.

- The senior leadership team will receive monitoring reports from the e-Safeguarding Coordinator.

- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious e-Safeguarding incident.

- The headteacher and senior leadership team should receive update reports from the incident management team

Responsibilities of the e-Safeguarding Coordinator

- To promote an awareness and commitment to e-Safeguarding throughout the school
- To be the first point of contact in school on all e-Safeguarding matters
- To take day-to-day responsibility for e-Safeguarding within school and to have a leading role in establishing and reviewing the school e-Safeguarding policies and procedures
- To lead the school e-Safeguarding group or committee
- To have regular contact with other e-Safeguarding committees, e.g. the local authority, Local Safeguarding Children Board
- To communicate regularly with school technical staff
- To communicate regularly with the designated e-Safeguarding governor
- To communicate regularly with the senior leadership team
- To create and maintain e-Safeguarding policies and procedures
- To develop an understanding of current e-Safeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in e-Safeguarding issues
- To ensure that e-Safeguarding education is embedded across the curriculum
- To ensure that e-Safeguarding is promoted to parents and carers
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To monitor and report on e-Safeguarding issues to the e-Safeguarding group and the senior leadership team as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safeguarding incident
- To ensure that an e-Safeguarding incident log is kept up to date

Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the e-Safeguarding coordinator
- To develop and maintain an awareness of current e-Safeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed e-Safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school

- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of technical staff

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any e-Safeguarding related issues that come to your attention to the e-Safeguarding coordinator.
- To develop and maintain an awareness of current e-Safeguarding issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted
- To be a member of the incident-management team that meets termly to review e-Safeguarding incidents that have occurred within school

Responsibilities of pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To help and support the school in the creation of e-Safeguarding policies and practices and to adhere to any policies and practices the school creates
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices
- To know and understand school policies on the taking and use of mobile phones
- To know and understand school policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home

- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss e-Safeguarding issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting e-Safeguarding
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school
- To sign a home-school agreement containing the following statements
- We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community
- Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school
- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.

Responsibilities of the Academy Council

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the e-Safeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its e-Safeguarding strategy

Responsibilities of the Child Protection Officer

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to e-Safeguarding and the safe use of technologies
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school.

Managing digital content

1 Using images, video and sound

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done annually or as part of the home-school agreement on entry to the school.

On the school website or blog
On the school's learning platform
In the school prospectus and other printed promotional material, e.g. newspapers

In display material that may be used off site
Recorded or transmitted on a video or via webcam in an educational conference

- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites (optional - unless appropriate security settings are enabled and set to maximum)
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

2 Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment. The school will store images of pupils that have left the school for 3 number of years following their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- Class Teachers are responsible for deleting images when they are no longer required, or when a pupil has left the school.

Learning and Teaching

The key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We acknowledge that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a series of specific e-Safeguarding-related lessons in every year group/specific year groups as part of the ICT curriculum / PSHE curriculum
- We will celebrate and promote e-Safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Child Line or the CEOP report abuse button

Staff training

- Our staff receive regular information and training on e-Safeguarding issues in the form of annual updates and termly staff meetings
- As part of the induction process all new staff receive information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-Safeguarding activities and awareness within their curriculum areas

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.

- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.
- All staff laptops are encrypted with 'Bitlocker' protection to limit access to data.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Pupils at Key Stage 1 will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords e.g. Do not write down system passwords.
- 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 as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.

- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.

Emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level.
- Emerging technologies can incorporate software and/or hardware products.
- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- All new technologies deployed within school will be documented within the e-Safeguarding and Acceptable Use Policies prior to any use by any member of staff or pupil.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the e-Safeguarding policy is adequate and that the implementation of the e-Safeguarding 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 the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by RM
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safeguarding Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.

- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.

- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Internet access authorisations

- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.
- Pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

Email

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils will be allocated an individual email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails 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. A full audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers, as approved by the senior leadership team and the Senior Information Risk Officer.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Staff to use encrypted email service when transferring any personal or confidential information using 'encrypt' in the body of the email.

Email usage

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Pupils must not reveal personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Pupils and staff should never open attachments from an untrusted source but should consult the network manager first.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- All pupils with active email accounts are expected to adhere to the generally accepted rules of netiquette; particularly in relation to the use of appropriate language. They should not reveal any personal details about themselves or others in email communication or arrange to meet anyone without specific permission.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within school should report any inappropriate or offensive emails through the incident-reporting mechanism within school.
- Pupils must immediately tell a designated member of staff if they receive any inappropriate or offensive email.

- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.
- Emails sent to external organisations should be written carefully and authorised before sending to protect the member of staff sending the email.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school'.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.
- When away for extended periods, 'out-of-office' notification should be activated so that colleagues are aware that you are not currently available.

Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

- Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform or school website.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website or an approved site and postings should be approved before publishing.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

Mobile phone usage in schools

General issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- 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.
- Personal mobile phones will only be used during lessons with permission from the Headteacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of personal devices

- Pupils should not bring his or her mobile phone or personally-owned device into school. Any device brought into school should be taken to the school office before registration . Mobile phones and devices which aren't handed in and are found to be in school will be confiscated and will be released to parents or carers in accordance with the school policy.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.
- Mobile Phones and personally-owned 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 granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a 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.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide their own mobile numbers for confidentiality purposes.

Data protection and information security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- All access to the school information management system will be on a need-to-know or least privilege basis.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- Fax machines will be situated within controlled areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Management of assets

- Details of all school-owned hardware and software will be recorded in appropriate audit with serial numbers recorded and stored securely.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include 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 overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Signe Chair of Governors

Signed Designated CP Officer/ Headteacher

Signed Deputy designated CP Officer/ Deputy Headteacher

Airedale Infant School
Acceptable Use Agreement Primary Pupils

Teacher **Class**

Please take a few minutes to read this agreement and discuss it with your child. If you are happy with the agreement could both you and your child sign below. Should you require further explanation, please do not hesitate to contact your child's class teacher.

- I will only use ICT in school for school purposes
- I will only use my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know who my teacher has approved.
- I will not tell other people my passwords for the Learning Platform, school network or for other learning websites.
- I will only open/delete my own files
- I will make sure that all ICT related contact with other children and adults is appropriate and polite
- I will not deliberately look for, save or send anything that could offend others
- If I accidently find anything inappropriate on the internet, I will tell my teacher immediately
- If I see anything I am unhappy with or I receive messages I do not like, I will tell my teacher immediately
- I will not give out personal details such as my name, phone number, home address or school
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult come with me
- I know that my use of ICT can be checked and that my parent or carer contacted if a member of school staff is concerned about my safety
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

Signed Parent/Carer
Signed Child
Date

Airedale Infant School

Staff Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school/academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school/academy* ICT 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, unless I have

permission to do so. Where these images are published (Eg on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies. In line with the Academy Code of Conduct
- 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.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school / academy*:

- When I use my mobile devices (laptops/tablets/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/academy* equipment. I will also follow any additional rules set by the *school/ academy* 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 use personal email addresses on the school/academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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/ academy 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, unless this is allowed in school/academy policies. I will not disable or cause any damage to school / academy 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/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- 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/academy 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.

When using the internet in my professional capacity or for school sanctioned personal use:

- 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 the *school/academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/ academy
- 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/Directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: ..... Date .....