



ICT AND E-AWARENESS POLICY

This policy should be read in conjunction with other policies including Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection, Copyright Protection and Freedom of Information policies.

Introduction

This policy aims to cover the different elements that Information Communication Technology (ICT) can cover within our school. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum, this policy will enable these to go ahead. This policy will set out a framework for how ICT will be taught, assessed and monitored throughout the school and should reflect the ethos and philosophy of our school. This policy has been written with guidance and support from other teachers, schools and local authorities and incorporates our eSafety and Social Media policies. Further information on the different systems in school will be made available to staff and pupils as and when new technologies and associated training are introduced.

Aims/Rationale

ICT encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent independent users and learners of ICT we aim:

- To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use ICT to help improve standards in all subjects across the curriculum
- To develop the ICT competence and skills of pupils using a cross-curricular context
- To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation

- To provide all staff with appropriate training and support to ensure that they can, and have the confidence to, use ICT to its full potential in all aspects of school life
- To use ICT as a form of communication with parents, pupils and the wider community

Curriculum

Computing will be taught across the curriculum and wherever possible, integrated into other subjects. Children will be taught Computing using a range of software and hardware including mobile technologies.

The ICT Subject Leader will ensure that curriculum plans provide coverage of the National Curriculum Programmes of Study for Computing and that children are challenged and are able to succeed.

In Reception, children will be taught how to use various pieces of ICT equipment, including the computers and technology rich resources, in accordance with the revised Early Years Foundation Stage Framework.

Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child. This will include recommended websites, open source software and use of Cloud technology for collaborative and remote working.

Assessment

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen across all curriculum areas and will be used to inform future planning and this is conducted by the teacher on an informal basis.

Moderation will take place with local schools through the ICT Subject Leaders' Network to ensure consistency. As part of our arrangements for reporting to parents, computing will be discussed where necessary as part of our parental consultations. Our annual reports will include a comment on children's Computing progress.

Some ICT skills will be taught through peer led sessions using our Digital Leaders. Children will also complete regular self and peer evaluations to review their progress and learning. Children's work will be stored in a personal folder on our network or in our password protected Dropbox (to be introduced Spring term 2013).

Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the Computing curriculum throughout the school. Where necessary, we will endeavour

to make adaptations to the environment or provide software that will enable all learners to achieve.

Roles and Responsibilities

The Head Teacher and ICT Subject Leader are responsible for monitoring the teaching of ICT and Computing throughout the school. Staff will work together to decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, ICT action plans and timescales.

Roles and Responsibilities - ICT Subject Leader

The ICT Subject Leader will oversee planning in all year groups throughout the school and be responsible for raising standards in ICT. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The ICT Subject Leader is responsible for overseeing the assessment of ICT across the school and providing opportunities to moderate ICT ability. They are responsible for keeping the hardware inventory up-to-date and ensuring the school has the appropriate number, and level, of software licenses for all software within the school. The ICT Subject Leader is responsible for managing equipment and providing guidance for future purchasing. The ICT Subject Leader is also responsible for ensuring tools and procedures are sustainable.

Roles and Responsibilities - Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach Computing and to use ICT within their class in accordance with Curriculum 2014. They will also assist in the monitoring and recording of pupil progress in Computing. Teachers should also respond to, and report, any e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below.

Whilst checking of personal sites - providing they are not blocked by the LA Firewall - e.g. email, is permitted during non-contact times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and ensure they are logged off appropriately. Staff should follow, and agree to, the Acceptable Usage Policy below.

Roles and Responsibilities - Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely. If either a visitor or governor wishes to have an account to log on to the school network, they should speak to the Head Teacher, ICT Subject Leader or School Office Manager.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the Internet and ICT can be used productively and safely. We will

always ensure that we provide children with the opportunities to excel and achieve when using ICT and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events. A range of e-safety websites will be made available on the school website.

From time to time we will conduct surveys of pupils to ascertain use of technology at home.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times. All children have signed an Internet Usage Agreement.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities - Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about e-safety and the use of the Internet. If they have any questions or concerns then they should speak to their child's teacher, the ICT Subject Leader or the Head Teacher. The school will run eSafety workshops for parents annually.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the Head Teacher and/or ICT Subject Leader. If staff use memory sticks then the school's antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the Head Teacher and/or the ICT Subject Leader for advice. The school reserves the right to examine or delete any files that are held on its system.

Staff are not given specific equipment but may borrow this as necessary providing this is signed in and out. To use the Internet at home, they will need to change the Internet settings as required and should seek advice from the ICT Subject Leader on how to do this if necessary.

Network

Staff will be issued with a username and password for the school system. Children currently log in using class log ins.

There are three levels of user on the system, FS/KS1, KS2 and staff. Each level has a different desktop and these are managed by the ICT Subject Leader. If teachers require different icons on the desktop, they should consult with the ICT Subject Leader.

The school has an Aruba wireless network. The password for this is available for staff on request. Staff may connect their own laptops to this network providing that the ICT Subject Leader has checked the laptop for sufficient virus protection software. If the password is provided on paper, it should be destroyed once it has been used.

School Website and Blogs - Linked to 360Safe Public Facing and Professional Standards Guidelines

The school website will be overseen by the ICT Subject Leader and Office Manager; it is expected that certain pages will be updated by other members of staff and children. Our website provision will be reviewed regularly. The school Twitter account is managed by the ICT Subject Leader and Office Manager. Updates needed should be directed to them

Internet and communications

The Internet may be accessed by staff and by children throughout their hours in school. As a school we sign up to the LA's Firewall and Anti-virus software which adds a significant level of security and protection to what children are able to access and view. However, no system is fail safe and we ask that staff are vigilant as to the sites children are accessing. Staff are made aware that they have greater access agreements than children and should, therefore, be vigilant about logging off when they are not in attendance.

The teaching of Internet use will be covered within the Computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the Internet.

The use of the Internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users see an inappropriate website or image, they should close this immediately and report the site to the Head Teacher/ICT Subject Leader who will take the necessary action as detailed by the LA.

School Liaison, Transfer and Transition

When a new child joins they will be provided with a network login and accounts for the online tools available.

Once they have left our school, the child's account will be removed from the online tools and their content will be removed. This will happen the year after they leave.

As a school we will make links with local schools to provide opportunities to aid the transition from one school to another. This will be monitored by the ICT Subject Leader.

Mobile Phones and Handheld Devices - Linked to 360Safe Mobile Phone Guidelines

Age Limits

Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13. Children are made aware of this through our eAwareness sessions.

Personal Data

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information on to personal devices unless strictly necessary. This data should then be removed as soon as possible. When using a personal laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display.

Social Media - Linked to 360Safe Social Media Guidelines

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community and just ask that these members of staff take extra precaution when posting online
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening

- Not use these media to discuss confidential information or to discuss specific children
- Check with the ICT Subject Leader if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.

We will use blogging throughout the school to share children's learning and to communicate with parents. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post on the blog or write a comment without it being approved by the ICT Subject Leader to ensure that the children are not subjected to any inappropriate comments. Spam messages (often containing inappropriate links and language) are caught by software installed on the blog and this is monitored by the ICT Subject Leader. This is also updated regularly.

As part of our surveys to parents and pupils, we will ask them questions on their use of social media to ascertain the number using sites such as Facebook as well as the popularity and usage of our blog. These discussions are also part of the everyday language of our school community and are approached openly and honestly without judgement.

Digital and Video Images - Linked to 360Safe Digital and Video Guidelines

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will try to ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to

the child's teacher or to the ICT Subject Leader. We will endeavour to remove the photograph as soon as possible

- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online

If staff use personal cameras or phones to take photographs of children within school, these should be removed from the device as soon as possible. We are fully aware that this is necessary at times, but precautions should be taken to minimise the risks.

Technical Support

Many minor issues are dealt with by the ICT Subject Leader and the Digital Leaders as appropriate.

Hardware technical support is provided by our technician when required.

Additional office-based support (e.g. MIS, SIMs) is provided by the North Yorkshire IT Helpdesk and forms part of the annual Service Level Agreement that the school has in place.

Sustainability and Environmental Impact - Linked to ICT Mark 1b4

To ensure that the level of ICT across the school is sustainable, the ICT Technician is responsible for the upkeep of usernames, passwords and guides to online tools and software as well as details of licenses and a complete ICT Inventory.

Hardware is disposed of safely and securely through a local company approved by North Yorkshire LA.

E-Safety - Linked to 360Safe E-Safety Guidelines

At Aiskew, Leeming Bar we take E-safety very seriously. We will ensure that it is taught often throughout the entire curriculum and in PHSCE as necessary. We will also provide children with dedicated e-safety lessons. These lessons and resources will come from Think U Know and there is a link for parents to this on the school website. Children will be taught how to act online and how to minimise the risk when working on the Internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

We will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual e-safety

focussed parent meeting and will provide regular updates via our website and newsletters as appropriate.

All children will be taught about the Internet Usage Agreement and will sign a copy related to their age phase. All staff have also signed the North Yorkshire LA Acceptable Use Agreements. This will be done at the start of each academic year.

E-safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online.

If there is a website available to children that staff or children deem inappropriate they should speak to the Head Teacher, ICT Subject Leader or School Office Manager who will then contact North Yorkshire LA to attempt to get this blocked.

If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the ICT Subject Leader and Head Teacher and recorded as appropriate.

If children receive any communication that they believe to be inappropriate then they should forward it on to their teacher and/or the ICT Subject Leader who will inform the Local Authority.

Complaints

Incidents regarding the misuse of the Internet by students will be delegated to the ICT Subject Leader who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the Head Teacher. Complaints of a child protection nature must be dealt with in accordance with child protection procedures. The Head Teacher is the designated Child Protection Officer for the school.

Copyright and Intellectual Property Right (IPR)

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the Internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the Internet. This could be as simple as putting the name of the site the image came from or a hyperlink. It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the Internet without some thought on their use.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This is in accordance with guidelines laid out North Yorkshire LA's Intellectual Properties Policy.

Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Responding to unacceptable use by pupils

Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

Acceptable Usage Policy - Staff - Linked to 360Safe AUP Guidelines

This document has been written to ensure that staff use the ICT throughout the school appropriately. If they have any questions regarding this policy, they should direct them to the Head Teacher or ICT Subject Leader.

Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer
- Make use of resources such as cameras and microphones but ensure that these are returned after their use. They should also endeavour to remove pictures/files on return too
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the ICT Policy
- Be aware that software or hardware should not be installed without prior consent of the ICT Subject Leader or Head Teacher
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Head Teacher
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical. Where staff are using their own digital equipment such as cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible

- Report any issues to the Head Teacher or ICT Subject Leader as soon as possible
- Return any hardware or equipment if they are no longer employed by the school

Signed _____ Print _____ Date _____

Acceptable Usage Policy KS2 Children - Linked to 360Safe AUP Guidelines

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, netbooks, iPads and everything else including cameras and other devices. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher.

- At all times, I will think before I click (especially when deleting or printing)
- When using the Internet, I will think about the websites I am accessing
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will keep my usernames and passwords secure
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

Signed (Pupil) _____ Class _____ Date _____

Acceptable Usage Policy KS1 Children - Linked to 360Safe AUP Guidelines

These rules have been written to make sure that you stay safe when using the computers. This includes cameras, netbooks, iPads and microphones too. By using the ICT in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher.

The Golden Rule: Think before you click

- ☺ I will be careful when going on the Internet.
- ☺ I will tell a teacher if I see something that upsets me.
- ☺ I know people online might not be who they say they are.
- ☺ I will be polite when talking to people or writing online.
- ☺ I will think before I print or delete.
- ☺ I will be careful when using or carrying equipment.
- ☺ I will keep my password secret, but I can tell my family.
- ☺ Remember to log off properly.
- ☹ I won't tell anyone any personal details like my phone number or last name.
- ☹ I won't logon using someone else's username.
- ☹ Never put water bottles on the table when using ICT.

Signed (Pupil) _____ Class _____ Date _____

Acceptable Usage Policy Governors and Visitors - Linked to 360Safe AUP Guidelines

Visitors, both physical and virtual, may be provided with accounts to our network and/or online systems. Visitors will have a lower level of access than staff and each account will be provided on a case-by-case basis. This will depend on the purpose of the account requested.

Users will:

- Not have access to mail or direct contact with children (unless strictly necessary)
- Understand that this account may be removed at any time so should not use it to save vital information

School Network and wireless

Users will:

- Be given a login for their time in the school
- Be expected to follow the guidelines as set out for staff
- Understand that this account may be removed at any time
- Be provided with the wireless key and guidelines for connecting to the network