E-safety Policy



2015

Tanner

Welholme Academy

**Policy 2014**

**Adopted:**

**Next review:**

**Background and rationale**

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few.

* Access to illegal, harmful or inappropriate images or other content.
* Unauthorised access to/loss of/ sharing of personal information.
* Risk of being subject to grooming by those with whom they make contact on the Internet.
* Sharing/distribution of personal images without an individual’s consent or knowledge.
* Inappropriate communication/contact with others, including strangers.
* Cyber –bullying.
* Access to unsuitable video/internet games.
* An inability to evaluate the quality, accuracy and relevance of information on the internet.
* Plagiarism and copyright infringement.
* Illegal downloading of music or video files.
* Potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, carers, friends and the wider community) to be aware and to assist in this process.

**Policy and leadership**

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT.

**Responsibilities of the e- safety committee**

Welholme Academy has an e- safety committee led by our Head teacher Mrs Turrell, and made up of senior leaders, staff, governors and pupils. It meets on a termly basis to:

* Review and monitor this policy
* Consider any issues relating to school filtering
* Discuss any e-safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school.

**Responsibilities: e-safety coordinator**

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e- safety coordinator:

* attends the e-safety committee as well as discussions on e-safety with the School Council.
* takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
* ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
* provides training and advice for staff.
* liaises with school ICT technical staff
* liaises with the Enquire Learning Trust and LA
* receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
* meets with e-safety governor to discuss current issues and review incident log
* attends relevant meetings and committees of governing body
* reports regularly to head teacher and Child Protection co-ordinator
* receives appropriate training and support to fulfil their role effectively
* has responsibility for passing requests for blocking/unblocking internet sites in the school’s filtering system.
* maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices.

**Responsibilities: governors**

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

* regular meetings with the E-safety Co-ordinator with an agenda based on monitoring: e- safety logs, filtering change logs, search and deletion of electronic devices logs.
* reporting to relevant Governors committee/meetings

**Responsibilities: head teacher**

The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator.

The head teacher and other members of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

**Responsibilities: classroom based staff**

Teaching and Support Staff are responsible for ensuring that:

* they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
* they have read, understood and signed the school’s Acceptable Use Policy for staff.
* they report any suspected misuse or problem to the E-Safety Co-ordinator.
* digital communications with students (email/Virtual Learning Environment (VLE)) should be on a professional level and only carried out using official systems.
* e-safety issues are embedded in the curriculum and other school activities.

**Responsibilities: ICT Officer**

The ICT Officer is responsible for ensuring that:

* the school’s infrastructure is secure and is not open to misuse or malicious attack.
* users may only access the school’s network through properly enforced password protection policy
* shortcomings in the infrastructure are reported to the e-safety coordinator or head teacher so that appropriate action may be taken.

**Policy development, monitoring and review**

This e-safety policy has been developed by a working group made up of:

School E-Safety Coordinator

Head teacher

Teachers

ICT Officer

Governors

Pupils

Schedule for development/monitoring/review of this policy

|  |  |
| --- | --- |
| The implementation of this e-safety policy will be monitored by: | The e-safety committee under the direction of the e-safety coordinator |
| Monitoring will take place at regular intervals: | Annually |
| The governing body will receive a report on the implementation of the e-safety policy generated by the e-safety committee at regular intervals: | Annually |
| The e-safety policy will be reviewed annually or more regularly in light of any significant development in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | July 2017 |
| Should serious incidents take place, the following external persons/agencies should be informed: | North East Lincolnshire Safeguarding Children Board, e-safety representative. |

**Policy Scope**

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when, they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

**Acceptable Use Policies**

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable user policy (AUP), which they will be expected to sign before being given access to school systems.

AUPs are provided in Appendix 1 of this policy for:

* Pupils (FS + KS1/KS2)
* Staff (and volunteers)
* Parents/carers (including permissions to use pupil images/work and to use ICT systems)

AUPs are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents/carers.

For parents/carers in FS and KS1 parents may sign on behalf of their children.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents/carers sign once when their child enters the school. The parents’ policy also includes permission for use of their child’s image (still or moving) by the school, permission for their child to use the school’s ICT resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year.

Induction policies for all members of the school community include this guidance.

**Self- Evaluation**

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school in particular the School Evaluation Form (SEF). The views and opinions of all stakeholders are taken into account as part of this process.

**Whole School approach and links to other policies**

This policy has strong links to other school policies as follows:

**ICT** How ICT is used, managed, resourced and supported in our school

**E-Safety** How we strive to ensure that all individuals in school stay safe while using ICT. The e- safety policy constitutes part of the ICT policy

**Anti-bullying** how our school strives to eliminate bullying – link to cyber bullying

**PSHE** E- safety has links to this – staying safe

**Safeguarding**  Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms part of the school’s safeguarding policy.

**Behaviour** Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

**Illegal or inappropriate activities and related sanctions**

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems ( in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

* **child abuse images (The protection of Children Act 1978)**
* **grooming, incitement, arrangement or facilitation of sexual acts against children (Sexual offences Act 2003)**
* **possession of extreme pornographic images (Criminal Justice and Immigration Act 2008)**
* **criminally racist material in UK – to stirrup religious hatred (or hatred on the grounds of sexual orientation) (Public Order Act 1986)**
* pornography
* promotion of any kind of discrimination
* promotion of racial or religious hatred
* threatening behaviour, including promotion of physical violence or mental harm
* any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

* using systems to run a private business
* use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
* uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without necessary licensing permissions
* revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access code and passwords)
* creating or propagating computer viruses or other harmful files
* carrying out sustained or instantaneous high volume network traffics ( downloading/uploading files) that causes network congestion and hinders others in their use of the internet
* on-line gambling and non-educational gaming
* use of personal social networking sites/profiles for non- educational purposes

If members of staff suspect that misuse might have taken place but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that school will need to deal with incidents that involve inappropriate behaviour rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

**Pupil sanctions – see Table 1**

**Staff sanctions – see Table 2**

**Use of hand held technology (personal phones and hand held devices)**

We recognise that the area of mobile technology is rapidly advancing and it is our school’s policy to review its stance on such technology on a regular basis. Currently our policy is:

Members of staff are permitted to bring their personal mobile devices into school. They are required to use their professional judgement as to when it is appropriate to use them. Broadly speaking this is:

* Personal hand held devices will be used in lesson time only in emergency or extreme circumstances.
* Members of staff are free to use these devices in school, outside teaching time.

Pupils are not currently permitted to bring their personal hand held devices into school and if they do they should hand them into the admin team for safe keeping.

**Use of communication technologies**

**Email**

Access to email is provided for all users in school. Pupils message through DB Primary and staff use google mail. These school email services may be regarded as safe and secure and monitored.

* Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access)
* Users need to be aware that email communications may be monitored
* Pupils have access to an individual email account for communication within school.
* A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
* Staff may only access personal email accounts on school systems for emergency or extraordinary purposes.
* Users must immediately report to their class teacher/ e-safety coordinator – in accordance with the school policy - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

**Video conferencing**

Video conferencing equipment in classrooms must be switched off when not in use and not set to auto answer.

External Internet Protocol addresses should not be made available to other sites.

Videoconferencing contact information should not be put on the school website.

Videoconferencing is supervised by a teacher.

Permission for pupils to take part in video conferences is sought from parents/carers at the beginning of the pupil’s time in school and only when granted may children participate.

**Use of digital and video images**

* When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own image on the internet e.g. on social networking sites.
* Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of these images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Pupils must not take, use, share, publish or distribute images of others without their permission.

See also the following section for guidance on publication of photographs.

**Use of school web-based publication tools**

* Our school uses the public facing website, [www.welholmeprimary.com](http://www.welholmeprimary.com), for sharing information with the community beyond our school. This includes celebrating work and achievements of children.
* All users are required to consider good practice when publishing content.
* Personal information should not be posted on the school website and only official email addresses should be used.
* Only pupils’ first names are used on the website, and only then when necessary.
* Detailed calendars are not published on the school website.
* Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
* Pupils’ full names will not be used anywhere on a website and never in association with photographs
* Written permission form parents or carers will be obtained before photographs of pupils are published on the school website.
* Pupils’ work can only be published with the permission of the pupil and parents or carers.

**Virtual Learning Environment (VLE)**

Class teachers and the ICT officer (school administrator) monitor the use of the VLE by pupils regularly in all areas, but with particular regard to messaging and communication.

Staff use is monitored by the school administrator.

User accounts and access rights can only be created by the school administrator.

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the VLE.

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

a) The user will be asked to remove any material deemed to inappropriate or offensive

1. The material will be removed by the site administrator if the user does not comply.
2. Access to the LP for the user may be suspended.
3. The user will need to discuss the issues with a member of SLT before reinstatement.
4. A pupil’s parent/ carer may be informed.

**Professional standards for staff communication**

In all aspects of their work in our school teachers abide by the **Teachers’ Standards** as described by the DfE. Teachers translate these standards appropriately for all matters relating to e-safety.

* Any digital communication between staff and pupils or parents/carers must be professional in tone and content.
* These communications may only take place on official (monitored) school systems.
* Personal email addresses, text messaging or public chat/social networking technology must not be used for these circumstances.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for teaching and learning. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process.

**Filtering**

**Introduction**

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Virgin Media and system managing it ourselves through the system manager Meraki, we are able to unify management and control of all mobile devices and desktop devices.

**Responsibilities**

The day to day responsibility for the management of the school’s filtering policy is held by the ICT officer and the e-safety coordinator (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering in line with the process outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, all changes to filtering must

* Be logged in the control log
* Be authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to class teachers/e-safety coordinator any infringements of the school’s filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programme or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

**Education/training/awareness**

Pupils are made aware of the importance of filtering systems through the school’s e-safety education programme.

Staff users will be made aware of the filtering systems through:

* signing the AUP (as part of the induction process)
* briefing in staff meetings, training days, email

Parents/carers will be informed of the school’s filtering policy through the Acceptable Use agreement and through the e-safety awareness sessions/ newsletters.

**Monitoring**

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

**Audit/reporting**

Logs of filtering change controls and of filtering incidents are made available to:

* the e-safety governor
* the e-safety committee

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

**E-safety education**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-safety education will be provided in the following ways:

* A planned e-safety programme will be provided as part of ICT, PHSE and other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
* Key e-safety messages will be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
* Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
* In lessons where Internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
* Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the pupils visit.

**Information Literacy**

Pupils will be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

* Checking the likely validity of the URL
* Cross checking references
* Checking the pedigree of the compilers

Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. They will be taught how to make best use of internet search engines to arrive at the information they require.

We use the resources on dB Learning and CEOP’s Think U Know site as a basis for our e-safety education.

**The contribution of the children to e-learning strategy**

It is our general school policy to require children to play a role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children’s experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning. Pupils also play a part in monitoring this policy.

**Staff training**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
* All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction.
* The E-safety Coordinator will receive regular updates through attendance at LA and Enquire trust training sessions and by reviewing guidance documents released by government departments.
* The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

**Governor Training**

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or child protection. This will be:

* Attendance at training provided by LA
* Participation in school training/information sessions for staff or parents/carers.

The e-safety governor works closely with the e-safety coordinator and reports back to the full governing body.

**Parent and carer awareness raising**

Many parents and carers have only limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children’s on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational divide” (Byron Report)

The school will therefore seek to provide information and awareness to parents and carers through:

* Letters, newsletters, website
* Parents evenings
* Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

**Wider school community understanding**

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone’s responsibility to keep children safe in the non-digital world.

Community users who access school ICT systems/website/VLE as part of the Extended Schools provision will be expected to sign a Community User AUP before being provided with access to school systems.

**Acceptable Use policy agreement templates**



**Acceptable use policy agreement – KS1 pupil**

**This is how we stay safe when we use computers:**

* I will ask an adult if I want to use a computer or an ipad.
* I will only use activities that an adult says.
* I will take care of the computer, ipad and other equipment.
* I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
* I will tell an adult if I see something that upsets me on the screen.
* I know that if I break the rules I might not be allowed to use the computers or ipads.

I understand these computer rules and will do my best to keep them.

My name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Year 1 Signed (child)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date:

Year 2 Signed (child)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date:



**Acceptable Use policy agreement – pupil (KS2)**

I understand that while I am a member of Welholme Academy I must use technology in a responsible way.

**For my personal safety:**

* I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
* I will keep my password safe and will not use anyone else’s (even with their permission).
* I will keep my own personal information safe as well as that of others.
* I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

**For the safety of others:**

* I will not interfere with the way that others use their technology.
* I will be polite and responsible when I communicate with others.
* I will not take or share images of anyone without their permission.

**For the safety of the school:**

* I will not try to access anything illegal.
* I will not download anything that I do not have permission to use.
* I will only use my personal ICT kit if I have permission and then I will use it within the agreed rules.
* I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
* I will tell an adult if I find any damage or faults with technology, however this may have happened.
* I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
* I will only use social networking, gaming and chat through the sites the school allows.

I understand that I am responsible for my actions and the consequences. I have read and understand the above and agree to follow these guidelines.

|  |
| --- |
| Name: |
| Year 3 signed |  | Date: |
| Year 4 signed |  | Date: |
| Year 5 signed |  | Date: |
| Year 6 signed |  | Date: |



**Acceptable use policy agreement – staff & volunteer**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

**For my professional and personal safety:**

* I understand that the school will monitor my use of the ICT systems, email and other digital communications.
* I understand that the school ICT systems are 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 in the e-safety policy.
* I will not disclose my username or password to anyone else, nor will I try to use anyone else’s username and/or password.
* I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the e-safety co-ordinator.

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

* I will not access, copy or 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.
* 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 images. I will not use my personal equipment to record these images, unless I have permission to do so.
* I will only use chat and social networking sites in school in accordance with the school’s policies.
* I will only communicate with 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 Enquire Learning trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

* I will only use my personal mobile ICT devices as agreed in the e-safety policy and then in the same way as if I was using school equipment. 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 my personal email address on the school ICT systems except in an emergency.
* I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
* I will not try to upload, download or access any materials which are illegal (child abuse images, criminally racist material, adult pornography covered by 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter settings, unless I have permission from the e-safety coordinator.
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school data protection policy.
* I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

* I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
* I understand that if I fail to comply with this AUP Agreement, I could be subject to disciplinary action. His could involve a warning, a suspension, referral to Governors and /or the Trust and dismissal.

**I have read and understand the above and agree to use the school ICT systems (both in and out of school) with these guidelines.**

|  |  |
| --- | --- |
| **Name:** |  |
| **Signed:** |  |
| **Date:** |  |



**Acceptable use policy agreement and permission forms – parent/carer**

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times. This Acceptable Use Policy is intended to ensure:

* That young people will be responsible users and stay safe while using ICT (especially the internet)
* That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission slip form below to show their support of the school in this important aspect of the school’s work.

|  |  |
| --- | --- |
| Child’s name: |  |
| Parent/carer name: |  |
| Parent/carer signature: |  |
| Date: |  |

**Permission for my child to use the internet and electronic communication**

As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has signed an Acceptable User Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that the children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child’s activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have any concerns over my child’s e-safety.

|  |  |
| --- | --- |
| Parent/carer signature: |  |
| Date: |  |

**Permission to use digital images (still and video) of my child**

The use of digital images (still and video) plays an important role in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The school will ensure that when images are published that the child cannot be identified by name.

As the parent/carer of the above pupil, I agree to the school taking and using digital images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events, where permitted, which include images of children I will abide by these guidelines in my use of these images.

|  |  |
| --- | --- |
| Parent/carer signature: |  |
| Date: |  |

**Permission to publish my child’s work (including on the internet)**

It is the school’s policy to publish the work of pupils by way of celebration. This includes on the internet via the school website.

As the parent/carer of the above child I give my permission for this activity.

|  |  |
| --- | --- |
| Parent’s signature; |  |
| Date: |  |

**Your agreement of consent will carry through the school. If your circumstances change it is your responsibility to inform the school.**

**Our school’s e-safety Policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.**

**Table 1 Pupil sanctions**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Refer to class teacher | Refer to e-safety coordinator | Refer to head teacher | Refer to police | Inform parents/carer | Warning | Further sanctions- Removal of internet /network access; exclusion |
| Deliberately accessing or trying to accessing material that could be considered illegal |  |  |  |  |  |  |  |
| Unauthorised use of non-educational sites during lesson |  |  |  |  |  |  |  |
| Unauthorised use of mobile phone/digital camera/other handheld device |  |  |  |  |  |  |  |
| Unauthorised use of social networking/instant messaging/personal email |  |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files |  |  |  |  |  |  |  |
| Allowing others to access school network by sharing username and passwords |  |  |  |  |  |  |  |
| Attempting to access the school network, using another pupil’s account |  |  |  |  |  |  |  |
| Attempting to access the school network, using the account of a member of staff |  |  |  |  |  |  |  |
| Corrupting or destroying the data of others users |  |  |  |  |  |  |  |
| Sending an email, text or instant message that is regarded as offensive, harassment, or of a bullying nature |  |  |  |  |  |  |  |
| Continued infringements of the above, following previous warnings and sanctions. |  |  |  |  |  |  |  |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school |  |  |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system |  |  |  |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  |  |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  |  |  |  |  |  |  |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act |  |  |  |  |  |  |  |

**Table 2 – Staff sanctions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Refer to head teacher | Refer to HR | Refer to police | Warning | Disciplinaryaction |
| Deliberately accessing or trying to access material that could be considered illegal |  |  |  |  |  |
| Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email |  |  |  |  |  |
| Unauthorised downloading or uploading of files |  |  |  |  |  |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account |  |  |  |  |  |
| Careless use of personal data e.g. holding or transferring data in an unsecure manner |  |  |  |  |  |
| Deliberate actions to breach data protection or network security rules |  |  |  |  |  |
| Corrupting or destroying data of other users or causing deliberate damage to hardware or software |  |  |  |  |  |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature |  |  |  |  |  |
| Using personal email/social networking/instant messaging/text messaging to carry out inappropriate communications with pupils |  |  |  |  |  |
| Actions which could compromise staff member’s professional standing |  |  |  |  |  |
| Actions which could bring the school into disrepute or breach he integrity of the ethos of the school |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system |  |  |  |  |  |
| Accidentally accessing offensive pornographic material and failing to report the incident |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  |  |  |  |  |
| Breaching copyright or licensing regulations |  |  |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions |  |  |  |  |  |