Whiston Junior and Infant School

Part of White Woods Primary Academy Trust

Engaging Minds Developing Lives

E-Safety Policy

(Incorporating Home School Agreement and
E Safety Acceptable Use Policy)

Reviewed by SLT: January 2017
Approved by the Governing Body: March 2017
Review Date: March 2018

Whiston Junior and Infant School Vision Statement

The school aims to **provide quality education** for children between four and eleven years of age. Our aim is to provide high standards of teaching and learning through:

- A rich, broad, balanced and creative curriculum which sustains the engagement of all learners.
- Operating an environment which is safe, healthy, caring and supportive for everyone.
- Encouraging self-reliance and pride in all achievements.
- Developing learning skills and a love of learning, including the ability to question, enquire and be independent in their approach to learning.
- Promoting the development of tolerance and respect for others, regardless of race, creed or gender and ensure that all learners have equality of opportunity.

Our Overall Philosophy-Mission Statement

Our vision for Whiston J & I School is one of high standards achieved through the creative nature of the curriculum offered. We have a learning culture of high and realistic expectations of everyone, children and adults alike. We believe that **active participation** in learning is crucial, engaging children as active participants in their learning, not simply recipients of knowledge. Children are not seen as vessels to be filled.

We provide opportunities for developing **divergent thinking, problem solving, creativity** and **independence** in order to promote **confidence, curiosity, resilience, risk taking and maturity**. There are many aspects of the educational process that we judge to be non-negotiable, views that we hold with a passion about children's education.

Policy introduction

Policy statements -*The following statements clarify the aims of our training and policy documentation*

- To set out the key principles expected of all members of the school community at Whiston Junior and Infant School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Whiston Junior and Infant 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.

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 eSafeguarding behaviour that takes place out of school. 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 cyber bullying, or other eSafeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Review and ownership

- The school has appointed an eSafeguarding coordinator who will be responsible for document ownership, review and updates.
- The eSafeguarding policy has been written by the school eSafeguarding Coordinator and is current and appropriate for its intended audience and purpose.
- The school eSafeguarding policy has been agreed by the senior leadership team and approved by governors.
- The eSafeguarding 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 eSafeguarding.
- All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

Communicating the policy

- Child friendly rules will be used (differentiated for FS2/KS1 & KS2)and support our policy for the children in school.
- Any amendments will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An eSafeguarding or eSafety module is included in the PSHE (Rotherham Healthy Schools), Citizenship and ICT curriculum covering and detailing amendments to the eSafeguarding policy.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- We endeavor to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used

Roles and responsibilities

Responsibilities of the school community

We firmly believe that eSafeguarding 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 (SLT)

The Head Teacher *is ultimately responsible for eSafeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be a joint responsibility of* the Head Teacher*, Assistant Head, Computing Coordinator and the School Business Manager.*

- The Head Teacher and senior leadership team are responsible for ensuring that suitable eSafeguarding training and advice is offered to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The senior leadership team will ensure that monitoring of eSafeguarding takes place
- The Head Teacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.
- The Head Teacher and senior leadership team should receive update reports regarding the incident management

Responsibilities of the e-Safeguarding Coordination team

- To promote an awareness and commitment to e-Safeguarding throughout the school.
- **The Head Teacher will be the first point of contact in school on all eSafeguarding matters**
- The Head Teacher/Assistant Head/School Business manager/Computing Coordinator will take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures
- To communicate regularly with school technical staff (RBT Schools Connect)
- To communicate regularly with the designated eSafeguarding governor
- To communicate regularly with the senior leadership team
- To create and maintain eSafeguarding policies and procedures
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that eSafeguarding education is embedded across the curriculum
- To ensure that eSafeguarding 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 eSafeguarding issues to the staff 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 eSafeguarding incident
- To ensure that an eSafeguarding incident log is kept up to date

Responsibilities of teachers and support staff

- To read, understand and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff **Acceptable Use Policy**
- To report any suspected misuse or problem to the eSafeguarding team
- To develop and maintain an awareness of current eSafeguarding 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 eSafeguarding 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 eSafeguarding 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 (RBT Schools Connect)

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding 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

Responsibilities of pupils

- To be kept up to date of incident-management issues in reviewing any eSafeguarding incidents that have occurred within school
- To be made aware of and adhere to the school pupil **Acceptable Use Policy** (age appropriate)
- To be involved through the scheme of work in promoting the policies and practices the school creates (posters, assemblies etc.)
- 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 and SMART technology e.g. SMART watches
- To know and understand school policies regarding cyber bullying
- 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 develop awareness 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 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 eSafeguarding

- 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 eSafeguarding 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**.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and website.

We will ask parents to sign the **Home School Agreement** which includes a statement about their use of social networks in situations where it could reflect on our school's reputation and on individuals within the school community.

We request our parents to support the school in applying the eSafety policy.

(See attached Home School Agreement Leaflet)

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's eSafeguarding 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 computing 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 eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy

Responsibilities of the Child Protection Designated Lead

- 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 including the implications given in the **Prevent Duty Government document (June 2015)** on identifying and protecting children **at risk of radicalisation.**
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyber bullying and the use of social media for this purpose

NOTE:

All new safeguarding policies including this e-safety Policy will automatically refer to new Safeguarding protocols, guidelines and implications as and when they are released by the Government. This includes the changes to 'Keeping Children Safe in Education' (Septmeber 2016) and the Prevent Duty (June 2015).

Responsibilities of other external groups

The school does provide advice to any child or family who may have internet related issues, however we do not give other organisations or bodies access to the use of our technologies, other than access to the website, which cannot be edited by anyone other than school staff. However, should external groups have access to school hardware in the future, the following statements will apply:

- The school will liaise with local organisations to establish a common approach to eSafeguarding 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 - Using images, video and sound

Written permission from parents or carers will be obtained before photographs of pupils are published on any of the platforms mentioned below. This will be done as an opt out as part of the home-school agreement procedures on entry to the school.

Possible Platforms where photos may be used:

- *The school website or blog.*
- *In the school prospectus and other printed promotional material, e.g. newspapers In display material that may be used around the school 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.

As part of our school Esafety curriculum we will regularly 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.

Pupils and staff will **only use school equipment** to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the Head of School provided that any media is transferred solely to a school device and **deleted from any personal devices**. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not online; such resources will not be published online without the permission of the staff and pupils involved.

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

When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

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 only store images of pupils that have left the school for a **maximum of 4 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.

The Head of School has the responsibility of arranging with IT support to delete images when they are no longer required, or when a pupil has left the school.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know 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 joint duty, alongside parents, to help prepare our pupils to safely benefit from the opportunities the internet and other technologies bring.

- As a school, we provide a series of specific eSafeguarding-related lessons in each year group as part of the ICT / PSHE curriculum
- We will celebrate and promote eSafeguarding through a programme of assemblies and whole-school activities, including promoting Safer Internet Day.
- We will discuss, remind or raise relevant eSafeguarding 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.
- Staff will model safe and responsible behaviour in their own use of technology during lessons
- 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 age appropriate end-user **Acceptable Use Policy** which will be displayed in classrooms.

- Pupils will be taught about the impact of cyber bullying 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 Childline or the CEOP report abuse button

Managing and safeguarding IT systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.
All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. head teacher and member of technical support.
The wireless network is protected by a secure log on which prevents unauthorised access.
New users can only be given access by named individuals e.g. a member of technical support.
We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by Rotherham LA. This ensures that all reasonable precautions are taken to prevent access to illegal content. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However, deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

Teachers are encouraged to check out websites they wish to use prior to lessons for the suitability of content.

Notices are posted in classrooms and around school as a reminder of how to seek help.

Access to school systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords. Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).

- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.

- All pupils have a unique, individually-named user account for access to IT equipment and information systems available within school. *(EYFS pupils may be the exception to this)*

- The school maintains a log of all accesses by users and of their activities while using the system in order to track any e-Safety incidents.

- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security

Using the Internet

We provide the internet to

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the DfE and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only.

E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school e-mail system is monitored and checked.
It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum pupils are taught about safe and appropriate use of email.

Under no circumstances will staff contact pupils, parents or conduct any school business using personal email addresses.

Publishing content online

E.g. using the school website, Learning Platform, blogs, wikis, podcasts, social network sites

School website:

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum:

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school wherever possible. Pupils will only be allowed to post or create content on sites where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

Using mobile phones

Use of **mobile phones by pupils is not permitted in school** or in school activities. Children are not permitted to bring a mobile phone to school.

If parents wish a child to have a mobile phone with them as a safety precaution (i.e.: going home alone) a letter should be sent to notify staff and the class teacher will be in charge of the phone throughout the school day.

Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. **(*In an emergency, where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.)***

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member we do not consider it a defence that the activity took place outside school hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyber bullying', will be considered a disciplinary matter.

The use of personal mobiles during school hours for staff is prohibited (except for authorised break and lunchtimes or for school related business). Staff mobile phones should be stored or locked away from children e.g. Staff room (locked at all times) or lockable cupboard in classrooms. If a member of staff has an exceptional circumstance for needing access to their mobile phone they must ask permission from their line manager or Head Teacher.

We make it clear to staff, pupils and parents that the Head Teacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

Using other technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an eSafety point of view. We will regularly review this eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Protecting school data and information

The school recognises its obligation to safeguard staff and pupil's sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The school is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

Pupils are taught about the need to protect their own personal data as part of their eSafety awareness and the risks resulting from giving this away to third parties. **Staff** are made fully aware of the contents of the **Information Security Guidance for Staff** which is included as part of this policy. Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with **encrypted USB memory sticks** for carrying sensitive data
- All computers or laptops holding sensitive information are set up with strong passwords
- Staffs are provided with appropriate levels of access to the school management information system holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow procedures for transmitting data securely and sensitive data is not sent via emailed unless encrypted
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Governors or School improvement officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies
- **Staff personal mobiles phones are stored or locked away from children e.g. Staff room (locked at all times) or lockable cupboard in classrooms/office; however, if your phone is needed on an occasion for an emergency please ask your line manager for permission.**

Management of assets

Details of all school-owned hardware and software are recorded in an inventory.

All redundant IT equipment is 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.

(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.)

Dealing with eSafety incidents

All eSafety incidents are recorded in the School eSafety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious eSafety incident, concerning pupils or staff, they will inform the eSafety Lead, their line manager or Head of School who will then respond in the most appropriate manner.

Instances of **cyber bullying** will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's eSafety Lead and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Safeguarding Procedures and Guidance will be followed.

Dealing with complaints and breaches of conduct by pupils:

Any complaints or breaches of conduct will be dealt with promptly

- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- **any online activity by a member of the school community which is likely to adversely impact on the reputation of the school**
- **accessing inappropriate or illegal content accidentally and failing to report this**
- **inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons**
- **sharing files which are not legitimately obtained e.g. music files from a file sharing site**

- **using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute**

- **attempting to circumvent school filtering, monitoring or other security systems**
- **circulation of commercial, advertising or 'chain' emails or messages**
- **revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission**
- **using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)**
- **transferring sensitive data insecurely or infringing the conditions of the Data protection Act, revised 1988**

The following activities would normally be unacceptable for all users; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve

- **accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time**
- **accessing non-educational websites (e.g. gaming or shopping websites) during lesson time**
- **sharing a username and password with others or allowing another person to log in using your account**
- **accessing school ICT systems with someone else's username and password**

- **deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else**

All new safeguarding policies including this e-safety Policy will automatically refer to new Safeguarding protocols, guidelines and implications as and when they are released by the Government. This includes the changes to 'Keeping Children Safe in Education' (July 2015) and the Prevent Duty (June 2015).

Whiston Junior and Infant School
Saville Road
Whiston
Rotherham
S60 4DX

28th September 2016

Dear Parents,
Please could you read, sign and return the following agreement relating to E-safety. As a school we address issues relating to being safe when using the Internet on a regular basis and it is a crucial part of our teaching and learning curriculum, however it is becoming increasingly important that that this is something which needs to be dealt with as part of a home/school partnership.

Yours Sincerely,

Mrs T. Angell.
(Head Teacher)

Please detach and return completed to school as soon as possible.

Parent Home school agreement form relating to E Safety and acceptable use

I will support the school stance in relation to the use of all ICT related equipment and technology.

As a school, Whiston J & I expects that parents will ensure that any images or videos taken during assemblies, concerts or sports afternoons are for personal use and that images will not be published on the internet, including social networking sites such as Facebook, or any similar sites, unless these images are solely of their own children.

Parents will ensure that they take a significant role in ensuring that the internet is controlled at home and not used inappropriately or deliberately by their child / children in order to upset any other child or family in any way.

Parents will support the school in ensuring that they closely monitor and supervise their child's use of the internet and that they encourage safe internet use within the home.

Signed _____ *Date* _____

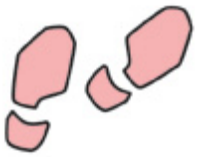
Parent of _____ *(Class Y …)*

Whiston J & I School Pupil Acceptable Use Policy (AUP)
Key Stage 1 Pupil agreement form

‘Think, then Click!’

These rules help us to stay safe on the Internet

I will only use the internet when an adult is with me.



I will only click on the buttons or links when I know what they do.

I will only search the Internet with an adult.

I will always ask for help if I get lost on the Internet.

I will only send and open emails when an adult is present.

I will only write polite and friendly emails to people that I know.

I, ……(Pupil name) in Year ……. agree to follow these rules above when using the Internet in school.

Child signature: Date:

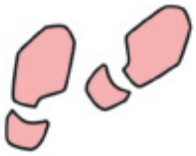
Whiston J & I School Pupil Acceptable Use Policy (AUP)
Key Stage 2 Pupil agreement form

‘Think, then Click!’

These rules help us to stay safe on the Internet

I will ask permission before using the Internet and will only use websites that an adult has chosen.

I will tell an adult immediately if I see anything that I am uncomfortable with, so that they can check it and take any necessary action.



I will only e-mail people an adult has approved.

I will send e-mails that are polite and friendly. I will ask my teacher to check them before they are sent.

I will never give out personal information or passwords.

I will not access other people’s files.

I will not bring USB flash drives or any other form of stored information to school.

I will never give my home address, phone number or arrange to meet someone.

I will not open e-mails sent by anyone I do not know and I will not use Internet chat rooms or social media sites at school.

I understand that the school may check my computer files and may monitor the Internet sites that I visit.

I, ……(Pupil name) in Year ……. agree to follow these rules above when using the Internet in school.

Child signature: Date:

Whiston J & I School Staff E-Safety Acceptable Use Policy (AUP) Acceptable Use Policy (AUP)

This policy covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school/LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- **I will only use the approved, secure email system(s) for any school business.**

  (This is currently: RGFL webmail)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network/Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I will access school resources remotely (such as from home) only through the RGfL/school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. (i.e. in a child protection situation)
- I understand I will never **use a personal mobile phone during work time unless authorised by my line manager or Head of school.**
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named child protection officer (Mrs T Angell/Mrs S Goodwin/Mrs J Furness) or a relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- **I understand that failure to comply with this agreement could lead to disciplinary action**.

Whiston J & I School Acceptable Use Policy (AUP): Staff agreement form

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

User Signature …… Date ……

Full Name (printed) _____

Job title _____

School **Whiston J & I School**

……

I (Head Teacher/Assistant Head/SBM) approve this user to carry on with a school email account or to be set-up with a new school email account.

Full Name (printed) _____

Role in School – see above ……..

Authorised Signature…… Date ……

(Signed of behalf of E-Safety Coordinating Team)

Additional Notes:

The annual Home School Agreement will also refer to e-safety.

A parent friendly information booklet '**Introduction to Safeguarding and e-Safety**' will be sent home annually to provide tips on managing risks, to highlight possible signs of child protection issues and to signpost further support through national and local agencies.

Teachers will discuss with the children all the statements in the **'Think, then Click!'** posters, to ensure they understand the importance of keeping themselves safe.

The following posters will be displayed and referred to during computing lessons or when accessing the Internet in all classes: **'Think, then Click!'**

All new safeguarding policies including this e-safety Policy will automatically refer to new Safeguarding protocols, guidelines and implications as and when they are released by the Government. This includes the changes to 'Keeping Children Safe in Education' (Sept 2016) and the Prevent Duty (June 2015).

Whiston J & I School
Foundation Stage 2 & Key Stage 1 e-Safety Rules

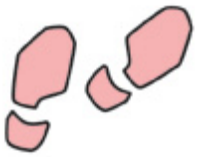
‘Think, then Click!’

These rules help us to stay safe on the Internet

We will only use the internet when an adult is with us.

We will only click on the buttons or links when we know what they do.

We will only search the Internet with an adult.



We will always ask for help if we get lost on the Internet.

We will only send and open emails when an adult is present.

We will only write polite and friendly emails to people that we know.

Whiston J & I School
Key Stage 2 e-Safety Rules

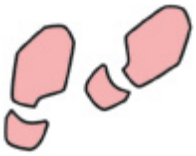
‘Think, then Click!’

These rules help us to stay safe on the Internet

We will ask permission before using the Internet and will only use websites that an adult has chosen.

We will tell an adult immediately if we see anything that we are uncomfortable with, so that they can check it and take any necessary action.

We will only e-mail people an adult has approved.



We will send e-mails that are polite and friendly. We will ask the teacher to check them before they are sent.

We will never give out personal information or passwords.

We will not access other people’s files.

We will not bring USB flash drives or any other form of stored information to school.

We will never give out our home address, phone number or arrange to meet someone.

We will not open e-mails sent by anyone we do not know and we will not use Internet chat rooms or social media sites at school.

We understand that the school may check our computer files and may monitor the Internet sites that we visit.