Rise Academy Online Safety Policy

Date Created: September 2015

Policy Creation and Review

This Online Safety Policy has been written as part of a consultaion process involving the following people and organisations:

Sue Yardley	Headteacher
Philip Mountain Wade	Strategic Commissioner & Safeguarding Senior Lead
Simone Butterworth	Chair – Management Committee
Netopian	

It has been reviewed by Management Committee and will be monitored and reviewed as listed below: Intended Policy Review – Date:

The implementation of this policy will be monitored by:
Philip Mountain Wade

This policy will be reviewed as appropriate by:
Philip Mountain Wade

Approved by: Sue Yardley (Headteacher) Date: Sept 2015
Approved by: Simone Butterworth (Management Committee) Date: Sept 2015

Contents **Page**

Appendices

Our vision for online safety

ICT is an increasingly essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. We recognise that all schools need to build on the use of these technologies in order to arm young people with the appropriate skills to access life-long learning and employment.

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

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones and tablets with text, video and/ or web functionality
- Other mobile devices and games consoles with web functionality

At Rise Academy we understand our responsibility to educate our pupils on 'online' issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the classroom environment. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote safe use of the online world.

Our vision is that pupils have a diverse, balanced and relevant approach to the use of technology, in an environment where security is balanced appropriately with the need to learn effectively. We aim to ensure that our children are equipped with the skills and knowledge to use technology appropriately and responsibly, that they understand the risks associated with this activity and are able to deal with these both in and out of school.

Rise Academy's Online Safety policy has been written to ensure safety measures are in place to protect both students and staff working with ICT equipment and related technologies. The policy is to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and students standards and practice. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to eSafety by knowing the content of the policy and the procedures adopted and developed by the school.

Scope of Policy

- This policy applies to the whole school community including Rise Academy's Senior Leadership Team, school Management Committee, all staff employed directly or indirectly by the school, commission partners and all pupils.
- Rise Academy's senior leadership team and school Management Committee will ensure that any relevant or new legislation that may impact upon the provision for Online Safety within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site. This is pertinent to incidents of Online bullying, or other Online related incidents covered by this policy, which may take place out of school, potentially at commissioned provision, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate Online behaviour that takes place out of school.

Review and Ownership

This Online Safety policy

- Has been written by the school Strategic Commissioner (Senior Lead for Safeguarding) in consultation with the Headteacher and the Child Protection Coordinator, and is current and appropriate for its intended audience and purpose.
- Has been endorsed and agreed by the senior leadership team and approved by the Management Committee.
- Will be reviewed annually or when any significant changes occur with regards to the technologies in use within the school.
- The School has appointed a member of the Management Committee to take lead responsibility for Online Safety.
- Amendments to the school Online Safety policy will be discussed in detail with all members of teaching staff and training will be given which will link to relevant and current guidance and legislation.

Responsibilities

We believe that Online Safety 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 list of responsibilities shows how each member of the community will contribute to the school vision

1. The Senior Leadership Team

- The head teacher is ultimately responsible for safeguarding provision (including Online Safety) for all members of the school community, with day-to-day responsibility for Online Safety delegated to the Senior Lead for Safeguarding (Philip Mountain Wade).
- The head teacher and senior leadership team are responsible for ensuring that the Child Protection Coordinator and other relevant staff receive effective and up to date training to enable them to carry out their Online Safety roles and to train other colleagues when necessary.
- The senior leadership team will receive updates from the Senior Lead for Safeguarding as appropriate.
- The head teacher and senior leadership team will ensure that procedures are rigorously followed in the event of all Online Safety incidents.
- The head teacher and senior leadership team will receive timely, regular and routine updates and reports on all Online Safety incidents.
- The team will ensure that Online Safety education is appropriately embedded across the whole curriculum.

2. The Senior Lead for Safeguarding and the Child Protection Coordinator

- Will promote an awareness and commitment to Online Safety throughout the school.
- To be the first point of contact in school on all Online Safety matters.
- Take day-to-day responsibility for Online Safety within school and to have a leading role in establishing and reviewing the school Online Safety policies and procedures.
- Have regular contact with other Online Safety committees, e.g. the local authority, Local Safeguarding Children Board (along with the Child Protection Coordinator).
- Will communicate regularly with the schools RM ICT technician, the designated Online Safety representative for the Management Committee and the senior leadership team.
- Will create and maintain Online Safety policies and procedures, reporting to the Management Committee at least annually.
- Will ensure that Online Safety is promoted to parents and carers.
- Liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
-

- Monitor and report on Online Safety issues to the senior leadership team as appropriate.
- Understand the issues surrounding the sharing of personal or sensitive information.

3. <u>Teachers and Support Staff</u>
   As a staff team we embrace modern technology but recognise that this is not a right but a responsibility, sanctions will be used if this expectation is misused

Are required to:

- Read, understand and actively promote the school's Online Safety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Agreement.
- Ensure that any Online Safety incidents are reported under appropriate escalation routes..
- Develop and maintain an awareness of current Online Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- 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, social networking etc. *Please see Social Networking guidance section 9. p14 of this document.*
- Embed Online Safety messages in learning activities across all areas of the curriculum.
- Supervise and guide pupils carefully when engaged in learning activities involving technology.
- Ensure that pupils are fully aware of research skills and methods.
- Be aware of Online Safety issues related to the use of mobile phones, cameras and handheld devices.
- Understand and be aware of incident-reporting mechanisms that exist within the school.
- Maintain a professional level of conduct in personal use of technology at all times.

<u>All Staff and Commissioned Partners</u>

Are required to:

- Be aware of the school's Online Safety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Agreement.
- Report any Online Safety related issues that come to their attention to the Senior Lead for Safeguarding or the Child Protection Coordinator. (Philip Mountain Wade or Munzella Hasan Ancliff)
- Develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in the use of technology at all times.
- Support the school in providing a safe technical infrastructure to support learning and teaching.

- Ensure that pupil access to the school network is only through an authorised, restricted mechanism.

4. Pupils *(Shared as part of the Admission Process)*
Are required to

- understand and adhere to the Acceptable Use Agreement
- Students who are unable to understand the AUP may require a parent/ guardian to sign on their behalf.
- Help and support the school in the creation of Online Safety policies and practices and to adhere to any policies and practices the school creates.
- Where appropriate pupils will be expected to understand school policies on the use of mobile phones, digital cameras and handheld devices.
- Know and understand school rules relating to bullying and Online bullying.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- 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.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exists within school.
- Discuss Online Safety issues with family and friends in an open and honest way.
- Through enrichment classes students can understands and contribute to the effectiveness of the Online Safety processes.

5. Parents and Carers *(Shared as part of the Admission Process)*
Are required to

- Help and support the school in promoting Online Safety.
- Read, understand and promote the school pupil Acceptable Use Agreement with their children.
- 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.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss Online Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

- Sign the photography permission form stating where photographs are to be published upon admission.

6. The Management Committee

Have agreed to

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance.
- Nominating one representative to have specific responsibility for Online Safety.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the internet by receiving regular reports at Management Committee meetings
- 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.
- Support the work of the Online Safety committee in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safety activities.

7. Child Protection Officer

Has a specific responsibility to:

- Have regular half termly meetings with SLT lead for safeguarding – review incidents and the schools response
- Understand the dangers regarding access to inappropriate online contact with adults and strangers.
- Be aware of potential or actual incidents involving grooming of young children.
- Be aware of and understand Online bullying and the use of social media for this purpose.

8. Other external groups

- Will receive a copy of this policy
- The school will liaise with other appropriate organisations to establish a common approach to Online Safety and the safe use of technologies.
- Any commissioned provision must reflect this policy in their organisations practices. The conditions of this policy is detailed in conjunction with their SLA
- 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.

Managing Digital Content

- Before photographs of pupils can be published, permission must be granted formally and agreed and signed by parents or guardians. All staff should be aware of the process involved with publishing images over different mechanisms.

- Parents and carers may withdraw permission, in writing, at any time. A procedure exists for permission to be removed retrospectively.
- The school 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 teacher provided that any media is transferred solely to a school device and deleted from any personal devices.
- 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.
- When searching for images, video or sound clips, staff 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.
- Individual staff members have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school. This instruction will come from a member of the Senior Leadership Team once a procedure and agreement has been decided.

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 duty to help prepare our pupils to safely benefit from the opportunities the internet brings. We recognise that three main areas of Online Safety risk as highlighted by OFSTED are:

1. Content – children and our communities need to be taught that not all content is appropriate or from a reliable source.
2. Contact – Children and stakeholders need to be made aware that digital technologies may be used as a vehicle for grooming, Online bullying and identity theft, and understand how to deal with these risks if they occur.
3. Conduct – Children and parents need to be aware that their personal behaviour on line and their electronic identity can increase the likelihood of, or cause harm to themselves and others. Key risk areas being disclosure of personal information, issues around sexting, privacy issues and copyright issues.

In order to minimise these risks to our pupils at Rise Academy

- We will discuss, remind or raise relevant Online Safety 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

- Deliver enrichment classes relating to personal safety which can be targeted to vulnerable individuals or groups
- 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.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Pupils will be taught about the impact of bullying and Online 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. This guidance will be coordinated through the Senior Lead for Safeguarding or the Child Protection Coordinator
- We will provide regular Online safety information to parents and carers, as well as hosting guidance on our website through CEOP and ParentInfo.

<u>Staff Training and awareness</u>

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

<u>Managing ICT Systems and Access</u>
(This will be managed by Rise Academy and RM)

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.

- Members of staff will access the network using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the network through their username and password. They will abide by the school AUP at all times.
- Permanent staff will agree removal and return of all e-media at their exit interviews
- All pupils, when appropriate, will have a unique username and password for access to ICT systems.

Passwords

- A secure and robust username and password convention exists for all system access.
- Staff should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Staff should change their passwords whenever there is any indication of possible system or password compromise.
- Pupils passwords will be managed by the appropriate member of support / teaching staff and changed when is deemed appropriate. Pupil passwords will be unique for all.
- Guest logins must be individually allocated and signed for at the main reception
- All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Staff are expected to comply with the following password rules;

1. Do not write down system passwords.
2. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
3. Always use your own personal passwords to access computer based services, never share these with other users.
4. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
5. Never save system-based usernames and passwords within an internet browser.

New technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an Online Safety point of view. We will regularly amend the Online Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an Online Safety risk.

- The school will audit ICT equipment usage to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

Mobile phones

- As a staff team we embrace modern technology but recognise that this is not a right but a responsibility; therefore students are allowed to have mobile devices however there use is not permitted during lessons without the agreement of the teacher
- If students fail to use their mobile device appropriately then a member of staff can remove their device
- Sanctions will be used if this expectation is misused

Staff use of Mobile Devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. All staff have access to either a school mobile phone or main line telephone
- Staff will use a school phone to contact parents or carers within the hours of the school opening times
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Filtering Internet Access

The school filters and monitors its internet provision appropriate to the age and maturity of pupils. – filtering is externally managed by Quickline (Internet provider) and RM (ICT facilities management)

- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Agreement and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafety Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Senior Lead for Safeguarding who will link with RM and Quickline. All incidents will be logged and chronologically recorded; the school will report such incidents to appropriate agencies including the filtering provider, the local authority or CEOP.
- The school will regularly review incidents through the Child Protection Coordinators meeting. All concerns can be highlighted to external contractors (RM and Quickline) in the contractual discussions.
- Pupils will be taught to assess content as their internet usage skills develop.

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

Internet Access Authorisations

- All parents will be required to sign a home-school agreement prior to their children being granted internet access in school. This consent is embedded in to a robust admission process whereby appropriate access, internet usage and Online safety is discussed and agreed prior to admission
- Parents will be asked to read the school Acceptable Use Agreement for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training through Online Safety briefing through the admission process and through lessons. All students are expected to sign the pupils Acceptable Use Agreement
- All staff will be offered Online Safety training, which will be updated annually, and sign the staff Acceptable Use Agreement. The school has a trained CEOP Ambassador (Strategic Commissioner) who will coordinate and deliver training.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign an Acceptable Use Agreement. Guest logins are available to those who have signed the acceptable use policy and are associated a personal 'guest' account
- All pupils will be supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

Email

Staff are required to comply with the following:

- Staff should only use approved email accounts allocated to them by the school and should be aware that use of the school email system is monitored and checked.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff are responsible for keeping their password secure.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.

- All emails that are no longer required or of any value should be deleted.
- Staff should check email accounts regularly for new correspondence.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within school should report any inappropriate or offensive emails through the Local Authority incident-reporting system.

Pupils are expected to:

- **Pupils are not issued with a school email address**

Use of Social Media

- Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.
- Staff and pupils are asked to report any incidents of Online bullying to the school.
- Staff will raise any concerns about pupil use of social media sites with parents/carers this includes the use of any sites that are not age appropriate.
- All staff will receive training on the risks associated with the use of social media either through staff meetings or via the induction process for new starters. Safe and professional behaviour is outlined in the Acceptable Use Agreement.
- Staff must not use social media tools to communicate with current or former pupils.
- Staff will not use any social media tools to communicate with parents.
- Procedures for dealing with Online bullying incidents of staff or pupils involving social media are outlined in the school Anti-Bullying policy.
- Staff are advised to set and maintain profiles on such sites to maximum privacy and to give access to known friends only.

Electronic Bullying and harassment

This Online safety policy recognises the additional dangers of Online bullying. All staff and pupils should be aware that any misuse of ICT to bully or harass others will be dealt with under the school Anti Bullying policy, and are reminded that:

‘Bullying is behaviour by an individual or group, repeated over time, which intentionally hurts another individual or a group physically or emotionally. Bullying can take many forms (for instance, cyber-bullying via text messages or the internet), and is often motivated by prejudice against particular groups (for example on grounds of race, religion, gender, sexual orientation, or because a child is adopted or has caring responsibilities). It might be motivated by actual difference between children, or perceived differences. Stopping violence and ensuring immediate physical safety is obviously a first priority but emotional

> bullying can be more damaging than physical. All staff will have to make their own judgements about each specific case.’

Dealing with incidents

All Online Safety incidents at Rise Academy are logged and recorded, with procedures regularly audited by the Head and Strategic Commission (SLT). Staff need to be aware of the following issues:

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Senior Lead for Safeguarding and the Head who will refer this to appropriate external authorities such as the Police, CEOP, Internet Watch Foundation or other agencies as appropriate. Examples of illegal offences are:

- Accessing Child abuse images
- Accessing criminally obscene content
- Inciting racial hatred
- Accessing sexual child abuse images and content

Staff should never under any circumstances investigate, interfere or share evidence of these activities as they may themselves be committing an illegal offence in doing so. Further information is available from www.iwf.org.uk.

Inappropriate use

Staff and pupils at Rise Academy are likely to have to deal with ‘accidental’ access to inappropriate materials and content. Examples of these and the actions and sanctions to apply are as follows:

1. Accidental access to inappropriate materials. Recommendation is to minimise the application, turn off the monitor. Pupils should tell a trusted adult. Staff will enter the details on the incident log, and advise the Senior Lead for Safeguarding to notify the filtering and monitoring company.
2. Using other peoples logins, accounts or passwords
3. Deliberate searching for inappropriate materials
4. Bringing inappropriate electronic media into school
5. Inappropriate use of chat and forums.
   Recommendation for each of the above is to inform the Child Protection Coordinator, enter the details onto the incident log, re-iterate and raise Online Safety issues with the individual or class, and for more serious or persistent offences consider disciplinary action and parent/ guardian involvement.

Evaluating the impact of this eSafety Policy

The SLT will regularly and routinely monitor and evaluate the impact of this policy by monitoring the number and range of Online Safety incidents in the school, regularly testing and checking on pupils awareness of Online Safety issues and looking for patterns and trends in practice.

The policy will be reviewed on an annual basis, with the support and oversight of the Management Committee. External agencies will be used to support this, to ensure current trends, new and emerging technologies and new threats to pupil safety are captured when the policy is refreshed.

Appendices

Appendix 1 – Image consent letter to parents
Appendix 2 – Image consent form
Appendix 3 – AU agreement for staff and Governors
Appendix 4 – AU agreement for Supply teachers, visitors and Guests
Appendix 5 – AU agreement for school pupils
Appendix 6 – AU letter to parents

Appendix 1 Image Consent Letter to Parents

Rise Academy
Fountain Road
Hull
HU2 0LH

t: 01482 226 166
e: admin@riseacademyhull.co.uk
www.riseacademyhull.co.uk

Dear Parent / Carer

As you may be aware we occasionally take photographs or videos of children at our school and believe that these can provide a valuable record of children's learning.

These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website, or in school displays, including digital photo frames.

We also actively encourage our children to use school cameras to take photographs or videos as part of their learning activity.

Occasionally, our school may be also be visited by the media or other organisations who may take photographs or videos of an event or to celebrate a particular achievement, for possible inclusion in in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse, and we endeavour to minimise risks by putting appropriate safeguards in place to protect your child's interests.

We also appreciate that some families may have additional concerns and needs to protect a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your consent.

I attach a consent form which needs to be completed for each child, and would appreciate you completing this and returning it to school as soon as possible. Should you require any further help or advice on this issue please contact the schools Senior Lead for Safeguarding – Philip Mountain Wade on 01482226166

Yours sincerely,

Headteacher

Appendix 2 Image Consent Form

Your Name **as the child's parent/carer**

Name of child:

Please read the following conditions of use, and then answer questions 1-4 before returning the completed form to school as soon as possible.

1. This form is valid for this academic year *<insert dates>.*

2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.

3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.

4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.

7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.

8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.

2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).

3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

Please Circle your response

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school?

   Yes / No

2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra-curricular events?

   Yes / No

3. May we use your child's image in printed school publications and for digital display purposes within school

   Yes / No

4. May we use your child's image on our school's online publications e.g. website / blog / VLE?

   Yes / No

5. May we record your child on video?

   Yes / No

6. May we allow your child to appear in the media as part of school's involvement in an event?

   Yes / No

I have read and understand the conditions on this form

Parent/Carer's signature:

Name (PRINT):

Date

Signed *(Parent / Carer)*

Print name

APPENDIX 3 ICT Acceptable Use Agreement for Staff and representatives of the Management Committee

ICT and the associated technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and MC representatives are aware of their individual responsibilities when using this technology. All staff members and MC Representatives are required to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

In signing this agreement you recognise that you will:

1. Take responsibility for your own use of any technologies, making sure that you use them safely, responsibly and legally.

2. Be an active participant in Online Safety education, taking personal responsibility for your awareness of the opportunities and risks posed by the use of technology.

3. Not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. Not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes inappropriate or inflammatory comments made on Social Networks, Forums and Chat rooms.

5. Not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. Respect copyright and intellectual property rights.

7. Ensure that all electronic communications with children and other adults are appropriate.

8. Not use the school system(s) for personal use during working hours.

9. Not install any hardware or software on school systems without prior permissions.

10. Ensure that personal data is kept secure at all times and is used appropriately in accordance with current Data Protection legislation.

11. Ensure that any images of children and/or adults will be taken, stored and used for legitimate purposes in line with school policy and with written consent of the parent/carer or relevant adult. You will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

12. Abide by the school’s rules for using personal mobile equipment, including my mobile phone, at all times.

13. Report any known misuses of technology, including the unacceptable behaviours of others.

14. Respect the technical safeguards which are in place. You understand that any attempt to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

15. Report failings in technical safeguards which may become apparent when using the systems and services.

16. Protect passwords and personal network logins, and will log off the network when leaving workstations unattended. You understand that any attempts to access, corrupt or destroy other users’ data, or compromise the privacy of others in any way, using any technology, is unacceptable.

17. Agree that network activities and online communications are monitored, including any personal and private communications made using school systems.

18. Note that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

19. Take responsibility for reading and upholding the standards laid out in the AU agreements. You will support and promote the school’s Online Safety policy and help children to be safe and responsible in their use of ICT and related technologies.

20. Understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action may be taken.

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

User Signature

Print

Appendix 4 ICT Acceptable Use Agreement for Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

3. I will not use any external device to access the school's network e.g. pen drive.

4. I will respect copyright and intellectual property rights.

5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

8. I will not install any hardware or software onto any school system.

9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

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

Signature

Date

Full Name (PRINT)

Position/Role

Appendix 5 Acceptable usage agreement school pupils

The school has installed computers with Internet access to help your learning. These rules will keep you safe and help us be fair to others.

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe;
- I will only access the system with the user identity and password given to me, which I will keep confidential;
- I will not access/delete other people's files;
- I will only use the computers for school work;
- I will not bring in CD's, memory sticks from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail people my teacher has approved;
- I will only open email attachments from people I know, or who my teacher has approved;
- I will only use my class email or own school address when emailing;
- The messages I send will be polite and responsible; I will not deliberately look for, save or send anything that could be unpleasant or nasty;
- I will not give my out my own personal details such as my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission and I am accompanied by an adult;
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

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

Signature

Date

Full Name (PRINT)

rise academy

Rise Academy
Fountain Road
Hull
HU2 0LH

t: 01482 226 166
e: admin@riseacademyhull.co.uk
www.riseacademyhull.co.uk

Appendix 8 ICT Acceptable Use Agreement – letter to parents

Dear Parent/Carer,

As I am sure you are aware, the use of ICT including the Internet, e-mail, learning platforms and mobile technologies are increasing elements of learning at Rise Academy.

To make this as safe, successful and as beneficial as possible for all our children, we expect our children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents should also check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate.

This is particularly important when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and we actively discourage this in our school.

The enclosed ICT Acceptable Use Agreement forms part of our wider School Online Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in this is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Agreement with your child and ensure they follow these basic rules to keep safe in the home as well.

If you would like to find out more about Online Safety for parents and carers, or if you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Philip Mountain Wade, Rise Academy, Senior Lead for Safeguarding.

Yours sincerely,