Newlands Junior School
We are Proud

Online Safety Policy and Acceptable Use of ICT

October 2024

Introduction

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy operates in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

Online Safety at Newlands Junior School: Writing and reviewing the policy.

The Policy relates to other policies including those for computing and for child protection.

- The school's e-safety Coordinator is also the ICT Coordinator. She works in close co-operation with the head teacher and Designated Child Protection Officers within school.
- Our Online Safety Policy has been written by the school. It has been agreed by the staff and governors.
- Online Safety issues are included in the Child Protection, Health and Safety, Anti-Bullying, PSHE and ICT policies.

Teaching and learning

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory computing curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
  Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

Sharing the Rules

Teachers will use an age-related and appropriate way of sharing the 'SMART' rules at Newlands Junior School. They will be introduced to children each year as part of the computing curriculum at the beginning of the school year and referred to regularly in teaching and learning time.

Cyberbullying – Our children have worked together to put together our schools procedures for dealing with cyber bullying.

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Details are set out in the school's policy on anti-bullying.

- Our children know how to report any incident of cyberbullying; to a responsible/ trusted adult and the matter will be dealt with immediately.
- Our children are aware of the support which is in place in school if anyone is affected by Cyberbullying.
- The victim and the child who has cyber bullied will be spoken to and their parents may be asked to come into school to speak about the incident and the sanctions which will be put in place following the cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Our children understand that there are procedures in place investigate incidents or allegations of Cyberbullying and that a copy of the bullying will be kept as evidence. Our children have agreed with our school sanctions for those involved in Cyberbullying which, depending on the incident, may include:
- A service provider may be contacted to remove content.
- Parent/carers may be informed and advised to contact the Police if a criminal offence is suspected.
- The child will be asked to remove any material deemed to be inappropriate or offensive if a teacher has not already done so.
- The child may have the electronic device they have used to cyberbully taken away from them or their access to school electronic devices restricted.

<u>Management of e-mail</u>

- Pupils may only use approved e-mail accounts on the school system. (Currently do not set up school emails for children to use)
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. ➢ The forwarding of chain letters is not permitted.

Management of published material

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school's website http://www.newlandsjunior.co.uk/ should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents/ carers will be obtained yearly for consent of pupil's images to be used in school/ on school publications/ media publications (local press) before images of pupils are published electronically.

Management of social networking and personal publishing

Whilst social media tools can provide tremendous benefits to individuals and education, they also have serious security risks in their use. Risks such as people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and exploit children.

The school will block access to social networking sites within school and will educate children through their e-safety lessons about the benefits and dangers of their own use of social media applications. Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils will be advised on what information is appropriate/ inappropriate to share online; they should always consider how public the information is. Advice and guidance on privacy settings on social media will be provided to children and parents through the schools website and at assemblies and workshops. Children will be shown age appropriate CEOP videos eliciting the potential dangers of social media app usage. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. House number, street name or school. Children will be made aware of their digital footprint and how their online activity can be monitored.

Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children will be made aware of the CEOP report button to report any unwanted/ inappropriate contact.

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator and a request for the site to be blocked will follow.

An e-safety incident log will be kept by the headteacher and e-safety co-ordinator to record ALL online incidents of an inappropriate nature, incidents will be recorded using CPOMs.

Managing emerging technology

Emerging technologies will be examined for educational benefit/ need and suitability before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. Mobile phones, if brought into school, must be handed in to the office prior to the start of the school day and may be collected at the end of the school day.
- Staff will not have mobile phones on their person during lesson times.
- The sending of abusive or inappropriate text messages is forbidden.

Authorised Internet access

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- Complaints of Internet misuse will be dealt with by the ICT co-ordinator and safeguarding team.
- Any complaint about staff misuse must be referred to the Head teacher.
- SMART rules will be displayed around school.
- Pupils will be informed that network and Internet use will be monitored.
- Online Safety is embedded across the curriculum to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.

Staff e safety awareness

- All staff will be given the School e-Safety Policy along with the Staff Acceptable Use agreement and its application and importance understood.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues. (See appendix for
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Community and parent awareness

- Parents' attention will be drawn to the school's online safety Policy in newsletters, assemblies, workshops the school and on the school website. Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- The parent section of the school's website includes an online safety section, which includes parental guides of advice and guidance for new apps and how they can monitor and manage their children's use of technology.

Newlands ICT Acceptable Use Policy

Newlands Acceptable Use Policy was developed and agreed by the staff and the Governing body. The policy was developed from the Nottinghamshire County Council's email and Internet code of practice and government guidance.

Purpose

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and children. Internet access is an entitlement for students who show a responsible and mature attitude.

Benefits

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between children world-wide;
- access to professional bodies and experts in many fields for children and staff;

Internet Content

The school Internet access is designed expressly for pupil use and will include high level filtering. The school will work in partnership with parents, the LA and the Internet Service Provider to ensure systems to protect children are reviewed and improved. Staff will guide children through safe online activities that will support the learning outcomes planned for the children's age and maturity.

Children will be educated in the effective use of the Internet. The school will where possible ensure that the use of Internet derived materials by staff and by children complies with copyright law. Older children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Safeguards

If staff or children discover unsuitable sites the URL (address) content must be reported to the Internet Service Provider via the ICT Subject Leader and it will be blocked from further viewing.

School Website

The point of contact on the school's website http://www.newlandsjunior.co.uk/ should be the school address, school email and telephone number. Staff or pupils' home information will not be published. Website photographs that include children will be selected carefully and will not enable individual children to be identified. Individuals will not be named in any photographs. Furthermore, pupils' full names will not be used anywhere on the website.

Parents are given the opportunity to state whether photographs of their child may or may not be published on the school website at the point of their child's admission to school. The school then acts on this information. The school will keep a record of all children who do not have consent for use of their photographs on the school website.

Cyberbullying – Our e safety committee have worked together to put together our schools procedures for dealing with cyber bullying.

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Details are set out in the school's policy on anti-bullying.

- Our children know how to report any incident of cyberbullying; to a responsible/ trusted adult and the matter will be dealt with immediately.
- Our children are aware of the support which is in place in school if anyone is affected by Cyberbullying.
- The victim and the child who has cyber bullied will be spoken to and their parents may be asked to come into school to speak about the incident and the sanctions which will be put in place following the cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Our children understand that there are procedures in place investigate incidents or allegations of Cyberbullying and that a copy of the bullying will be kept as evidence.
- Our children have agreed with our school sanctions for those involved in Cyberbullying which, depending on the incident, may include:
    - A service provider may be contacted to remove content.
    - Parent/carers may be informed and advised to contact the Police if a criminal offence is suspected.
    - The child will be asked to remove any material deemed to be inappropriate or offensive if a teacher has not already done so.
    - The child may have the electronic device they have used to cyberbully taken away from them or their access to school electronic devices restricted.

See e-safety incident log (appendices)

Emerging Internet Uses

Emerging technologies will be considered for educational benefit before use in school is permitted.

Internet Access Authorisation

The school allows Internet access to all staff and children. Initially access to the Internet will be introduced by adult demonstration with supervised access to specific, approved online materials. Children will be taught to use the Internet safely and effectively throughout their computing and embedded e safety lessons.

Inappropriate Material

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material suggesting appropriate sites and searches. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Our children are aware of our think before you click policy which they should follow whenever they use the internet and should inform a teacher or a trusted adult if they are aware of any inappropriate material so that this can be removed as soon as possible.

Passwords

- Users will only use their own account to carry out day to day work;
- Users will not disclosing their password to allow others to access their account.

- Users are aware passwords are for the benefit of the school and are the proprietary and confidential information of the school;
- The ICT co-ordinator will establish set individualised passwords for each child to access learning platforms used in school such as: Purple Mash, Spag.com, satsbootcamp, read theory, TTrockstars, prodigy maths. Children must only use their own password to access their own accounts and must never reveal their password to another pupil.

Staff

All staff including teachers, supply staff, teaching assistants, support staff and administrative staff will have access to the Staff Acceptable Use Policy (See appendix). Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Misuse of the ICT provision in school could lead to a formal disciplinary procedure being initiated.

ICT system security

The school ICT systems will be reviewed regularly with regard to security and any LA guidance will be adopted. The use of data sticks and any other data recordable devices, except by staff or with their expressed agreement, will not be allowed. Only authorized technicians will be able to introduce and install new programs onto the network.

Complaints

Responsibility for handling incidents will be delegated to a senior member of staff. Any complaint about staff misuse must be referred to the Head teacher. Parents will be informed should a pupil misuse the Internet and sanctions will be applied accordingly.

Parents

Information and support for parents can be found on the school website under the parents section where parental guides will be added for emerging apps and technologies to keep parents informed of how to keep their children safe.

Information and guidance can also be found at:

http://www.parentscentre.gov.uk/

www.thinkuknow.co.uk http://ceop.police.uk/

www.childnet.com/resources/know-it-all-for-parents www.nspcc.org.uk/onlinesafety

Review

This policy will be reviewed annually because of the ever-changing nature of the subject.

Appendix 1 :

Teaching e-safety awareness across the curriculum

Our newly designed curriculum has been created with our children's views and their parents' views in mind. After listening to what our children and parents felt was important to learn in e-safety, we created our skills progression to ensure progressive e-safety skills are taught through cross-curricular links during our redesigned topics for each year group; linking with our values, personal development and computational thinking and learning. Through our IT curriculum, teachers will deliver e safety and digital literacy lessons that promote children's personal development.

- developing pupils' character, defined as a set of positive personal traits, dispositions and virtues that informs their motivation and guides their conduct so that they reflect wisely, learn eagerly, behave with integrity and cooperate consistently well with others. This gives pupils the qualities they need to flourish in our society.
- developing pupils' confidence, resilience and knowledge so that they can keep themselves mentally healthy.
- enabling pupils to recognise online and offline risks to their well-being – for example, risks from criminal and sexual exploitation, domestic abuse, female genital mutilation, forced marriage, substance misuse, gang activity, radicalisation and extremism – and making them aware of the support available to them
- enabling pupils to recognise the dangers of inappropriate use of mobile technology and social media. Personal development will developed through children learning about permission and consent, feedback and comments on social media. Children will learn about the importance of developing a positive digital footprint and how their online reputation can affect their lives in terms of job prospects and that their online choices have consequences. They will learn how to give positive feedback and comments on work of their peers through the use of seesaw. Children will show the confidence to select the appropriate technology, program or app to complete a given task. They will also learn about their screen time and how they can manage this, developing a knowledge of the link between excessive screen time and the effect on mental health.

Online safety and digital literacy

- **Use technology purposefully, effectively, safely, respectfully and responsibly; keeping personal information private.**
- **Recognise acceptable/unacceptable behaviour;**
- **Identify a range of ways to report concerns about content and contact.**

In the teaching of E-safety, teachers will use age-appropriate content and will make use of online websites and resources to teach progressive skills across the key stage.

(CEOP, Think U know, CBBC, NSPCC, Childnet, NOS resources, Safetynet, KidSmart)

NC statement: Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Newlands Junior School progression of skills in E-Safety learning			
Year 3	Year 4	Year 5	Year 6
Recognise age appropriate games and websites	Choose age appropriate websites, apps and games	Make considered choices about accessing information on line, understanding that not everything is valid or safe	Be aware of the consequences of sharing too much personal information on line, and take steps to minimise risk
Know how to respond if contacted via on line technologies	Know that information shared on line can be accessed by others	Appreciate the protocols regarding respectful communication	Understand the consequences, to self and others, of unacceptable communication
Use the safety features of websites, reporting concerns to an adult	Use safety features of websites, reporting concerns when appropriate	Explain the need to protect themselves, and others, on line and the best way to do this, including reporting concerns to an adult	Support others to protect themselves and make good choices online, including reporting concerns to an adult

<u>Appendix 2 :</u>

<u>Primary Pupil : Acceptable Use Agreement and e-safety Rules</u>

<u>Parents and children must sign Newland's acceptable use agreement, which is provided in each child's homeschool diary, at the beginning of each new school year.</u> ✓ I will only use ICT in school for school purposes.

- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

Dear Parent / Carer

ICT and computing, including the internet and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these e-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Miss Coupe.

Primary Pupil Acceptable Use Agreement / e-safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

✂--

Parent/ carer agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, e-mail and on-line tools.
- I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy. I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to encourage safe and responsible use.

- I will be responsible for dealing with issues that arise whilst using the Internet at home. However, if I feel that these matters are having an impact on school life, I will make the school aware of these. I understand that if my child / children or staff become aware of issues that they feel are having an impact on school life, they may bring these to my attention.

Parent/ Carer Signature …….. Class ……

Appendix 3:

Newlands Junior School E-Safety Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the e-safety co-ordinator. This incident log will be monitored termly by the e-safety co-ordinator and Head teacher.

Date and name of pupil	Male or Female	Room/computer device number	Details of incident (including evidence)	Actions and reasons

Appendix 4:

Newlands Junior School filtering and monitoring log

In instances where a webpage/ internet content has needed to be blocked it will be recorded here and tests will be completed termly to ensure the content can no longer be accessed through school devices.

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Date and name of pupil	Room/computer device number	Details of incident (including evidence)	Actions and reasons	Reported to/ Date blocked

Appendix 5 – Staff Acceptable use policy

Staff Acceptable Use Policy

Newlands Junior School recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for ICT to enhance development in all areas of the curriculum and school administration. It is also recognised by that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate materials. In addition to their normal access to the school's ICT systems for work-related purposes, the school permits staff reasonable personal use of ICT equipment and e-mail and internet facilities during their own time subject to such use:

- not depriving pupils of the use of the equipment and/or
- not interfering with the proper performance of the staff member's duties

Whilst the school's ICT systems may be used for both work-related and for personal reasons the school expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the School at all times. The use of computer equipment, including laptop computers which is on loan to staff by the school for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy.

GUIDANCE ON THE USE OF* ICT FACILITIES *& THE INTERNET

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the school. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action.

E-mail and Internet usage

I will only use the approved, secure email system(s) for any school business, this is currently: Office 365. The following uses of the school's ICT system are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

1. to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it 2. to gain access to, and/or for the publication and distribution of material promoting racial hatred
3. for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation.
4. for the publication and/or distribution of libellous statements or material that defames or degrades others 5. for the publication and distribution of personal data without either consent or justification
6. where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination 7. to participate in on-line gambling
8. where the use infringes copyright law
9. to gain unauthorised access to internal or external computer systems

(commonly known as hacking)

10. to enable or assist others to breach the schools expectations as set out in this policy

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

1. for participation in "chain" e-mail correspondence
2. in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives)
3. to access ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.

Use of School ICT Equipment – users of school equipment:

1. must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries

2. must report any known breach of password confidentiality to the Headteacher or nominated ICT leader as soon as possible

3. must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems

4. must comply with any ICT security procedures governing the use of systems in the school, including antivirus measures.

Digital Communication

1. Digital communication received from pupils to any staff member must not be replied to, except when used as part of teaching about digital communication via the agreed means. Emails, messages or friend requests received through any social media platform must be reported to the school e-safety co-ordinator via an e-safety report form. (incident form in appendices)
2. Communication between staff members must be professional and appropriate. Staff should be mindful that electronic communication can be requested under the Education Act (2011) and that the act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. Any inappropriate communication will result in staff becoming subject to school disciplinary proceedings.

Social networking & Internet Use

1. You should not disclose confidential information relating to your employment
2. Sites should not be used to verbally abuse staff or students. Privacy and feelings of others should be respected at all times. You should obtain the permission of individuals before posting pictures. Care should be taken to avoid using language which could be deemed as offensive to others.
3. If information on a site raises a cause for concern with regard to conflict of interest, you should raise the issue with the head teacher
4. Sites must not be used for accessing or sharing illegal content
5. Staff will not make comments or upload photographs of children to any social network site or public arena of the internet, unless authorised to do so (in the case of school website/school twitter account/online competitions).
6. Staff are advised to keep any online profiles private and to check the privacy settings on their social networking profiles regularly, as they can change.
7. I will not engage in any online activity that may compromise my professional responsibilities. **Usernames and passwords**

1. All staff are advised to use impersonal appropriate usernames and strong passwords including a range of upper case, lower case, numbers and symbols.
2. Staff must use reasonable measures to ensure passwords are kept private and are changed regularly.
3. Staff muse ensure passwords provided by the school to access confidential information, such as children's names, are kept private and ensure they log out of such websites when not in use.

Images/Blogs/School Facebook Account

1. Staff are to use school-owned devices for capturing, recording and storing data/photos of children.
2. Names and personal details of children will not be published in public areas of the internet. Staff should note which children in their classes have permission for their photograph to be used in all, some or no school media publications.
3. Comments will relate to events at school and to show case children's learning.

General

- 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. **Reporting**

Any accidental access to, or receipt of inappropriate materials, or filtering breach will be reported to the esafety lead. Any incidents of staff misuse should be reported directly to the head teacher, or in their absence to the deputy head teacher.

Acceptable Use of ICT Agreement for Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- ✓ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- ✓ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- ✓ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- ✓ I will not give out my own personal details, such as mobile phone number and personal email address, to pupils
- ✓ I will only use the approved, secure email system(s) for any school business.
- ✓ I will ensure that personal data (such as data held on Scholar Pack) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- ✓ I will not use or install any hardware or software without permission from the computing/ e safety lead.
- ✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ✓ Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- ✓ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.
- ✓ I will respect copyright and intellectual property rights.
- ✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- ✓ I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- ✓ I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school. **User agreement:**

Signature …….…… Date ……

Full Name ……..... (printed) Job titile: ……