Kirkoswald CE School

Whole School E-Safety Policy

Issue No	Author	Date approved	Review date	Name	Position	Authorised signature
1	Governing Board	November 2019	November 2021	M Bowman	Chair	M.M. Bowman
2	Governing Board	January 2022	January 2024	Mark Bowman	Chair	M.M. Bowman
3	Finance, Premises, Health and Safety Committee	27th February 2024	February 2026	Andrew Hodgkinson	Vice Chair	A Hodgkinson

<div align="center">

Kirkoswald CE School
E-Safety Policy

</div>

General statement

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children, and adults responsible for them, about the *benefits* and *risks* of using new technology and provides *safeguards* and *awareness* for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Teaching & Learning and Data Protection.

Good Habits

- E-Safety depends on effective practice at several levels:
- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Operating to National Education Network standards and specifications (www.nen.gov.uk/esafety)

Kirkoswald CE Primary School acknowledges the assistance of National Education Network Safeguarding Group & Sheffield Children and Young Peoples' Directorate in providing content in this document.

School e-Safety Policy

Our e-Safety Policy is based on the Sheffield Children and Young Peoples' Directorate and Government guidance. It has been agreed by the Headteacher and teaching/management team and approved by governors.

The e-Safety Policy will be reviewed bi-annually.

Why is Internet Use Important?

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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. Our **pupils** are required to learn how to *locate*, *retrieve* and *exchange* information using ICT. At Kirkoswald CE Primary School we also believe that ICT supports creativity and adventure learning (e.g., producing talking books, making videos or using digital cameras and photo manipulation software). Our **teachers** need the internet to plan, to integrate web-based resources in delivering the curriculum and make full use of e-mail to communicate with support services, professional associations, and colleagues at all levels to ensure effective management.

ICT is an essential element in 21st century life for education, business, and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils world-wide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations

- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority and DfE
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?
- Kirkoswald CE School Internet access is designed specifically for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are 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.
- Staff should guide pupils in on-line activities that will support 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.
- Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Any adult taking responsibility for children using the Internet must do so in the full knowledge of information contained in this document.

Authorised Internet Access
- Kirkoswald CE School will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource including all supply staff, agency staff and Out of School Club staff.
- No child will use the Internet without a teacher or responsible adult giving permission.
- Internet access is only available during lesson times – computers are not an option during wet playtimes or lunchbreaks.
- Parents will be informed that pupils will be provided with supervised Internet access and regular teaching in how to be NETSMART both at home and at school.
- Parents will be asked to sign and return an annual consent form for pupil access to the internet
- and consent for use of images on the school's website.

World Wide Web
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator or Cumbria Software Services (Tel: 0871 423 8801) for inclusion in the list of blocked sites.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email
- Pupils may only use approved e-mail accounts on the school system – although it should be noted that **pupils DO NOT currently have their own accounts**
- 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.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked. Currently, MSN and Hotmail accounts are accessible, but it should be noted that **children DO NOT have permission to access any external e-mail accounts from school.**
- 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.

Social Networking
- School will block/filter access to social networking sites and newsgroups.
- Pupils will be advised **NEVER to give out personal details** of any kind which may identify them or their location (e.g., full name, address, telephone number, e-mail, or name of the school that they attend)
- Pupils will be advised **NOT to place personal photos on any social network space.**
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals, and instructed how to block unwanted communications. Pupils should be encouraged to **invite known friends only and deny access to others**.

Filtering and Monitoring
Kirkoswald CE School works in partnership with Cumbria Software Services, to ensure filtering and monitoring systems are as effective as possible.
The designated safeguarding lead takes lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place.
Filtering and monitoring provision will be reviewed at least annually.

Managing Emerging Technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time (including school trips and residential visits). The sending of abusive or inappropriate text messages is forbidden.
- Staff will carry a mobile phone and the school's text messaging system will be employed where contact with pupils is required.

Published Content and the School Web Site
- The contact details on the Web site should be the school address, e-mail, and telephone number. Staff or pupil's personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Annual written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupils' names will NOT be used anywhere on the Web site or Moodle, particularly in association with photographs.
- Work can only be published with the permission of the pupil and their parents- data and parental permission to be requested annually.

Information System Security
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with Cumbria Software Services

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the May 2018 GDPR regulations which replaced the Data Protection Act 1998.

Assessing Risks
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Cumbria County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints
- Complaints of Internet misuse will be dealt with by the headteacher.
- Any complaint about staff misuse must also be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

**Communication of Policy**
Pupils
- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- KS1 and KS2 e-safety awareness sessions will be facilitated by Class Teachers on an annual basis
- Y5/6 children will be provided with/and involved in producing guidelines for online safety at home and at school.

Staff
- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will receive training appropriate to their role on cyber security and online safety. Safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning
- All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
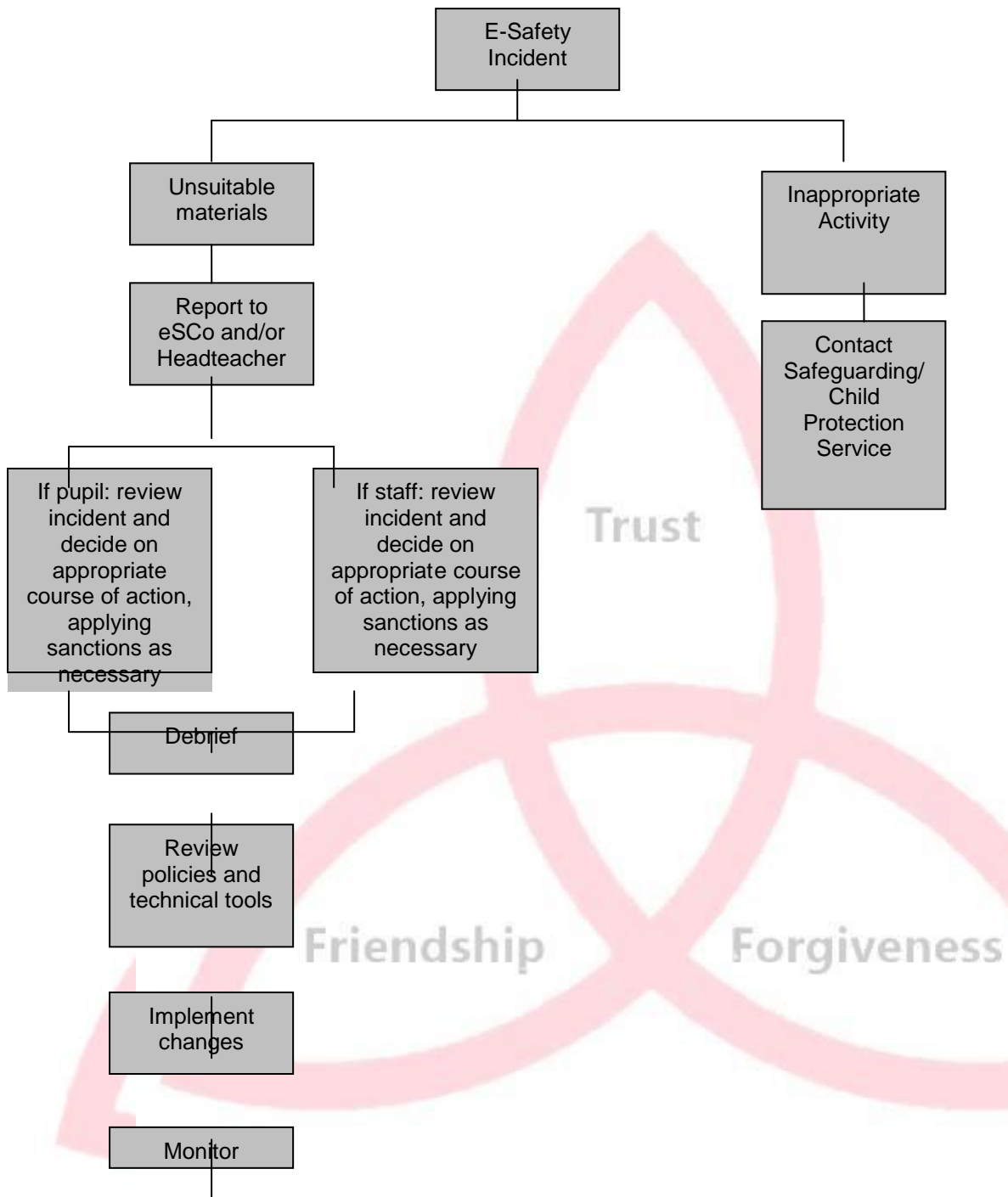
Parents
- Parents' attention will be drawn to the School e-Safety Policy in newsletters, posters, on display boards and on the school Web site.
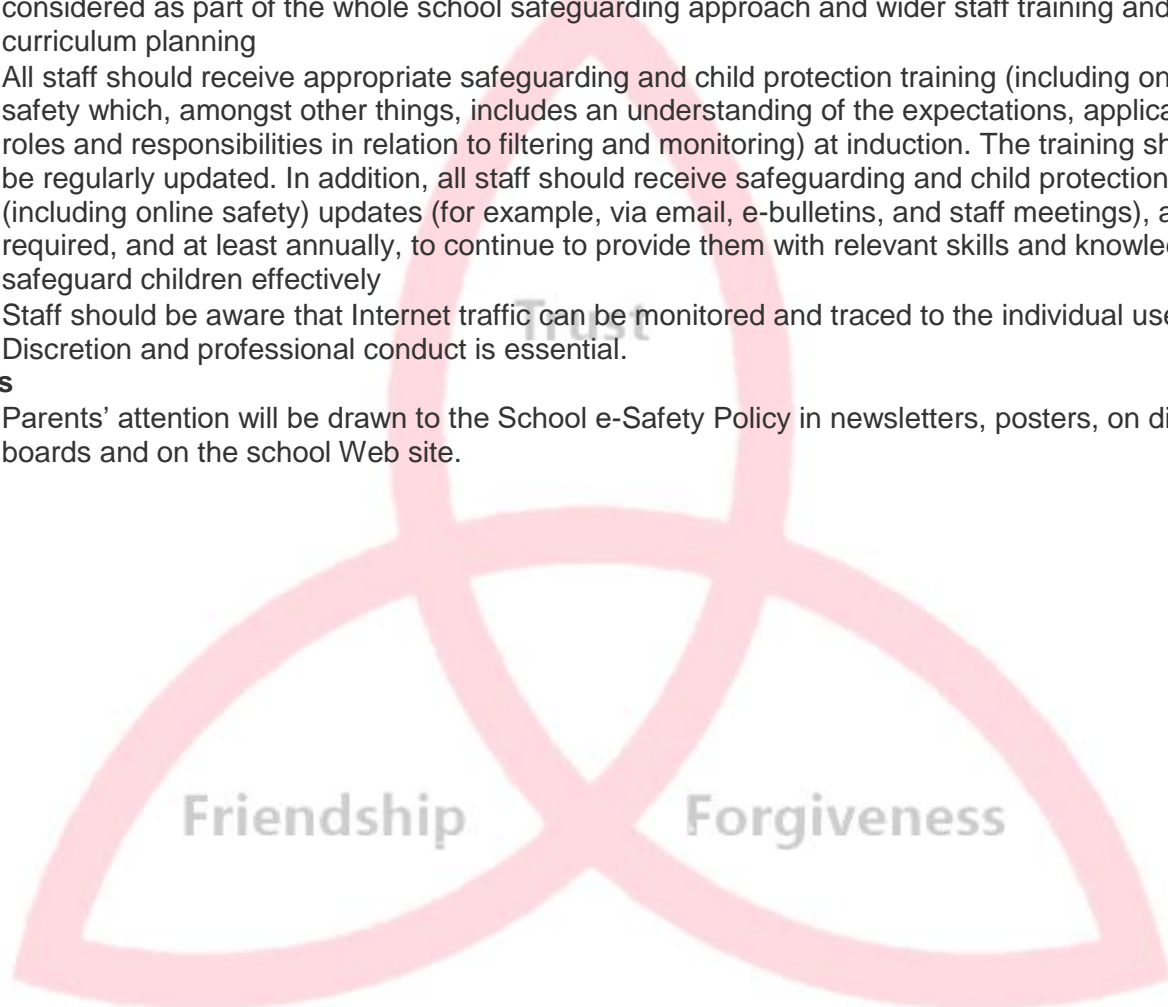
Appendix A

Flowchart for responding to e-safety incidents in school

```
                          ┌──────────────────┐
                          │    E-Safety      │
                          │    Incident      │
                          └──────────────────┘
                    ┌───────────────┴──────────────────┐
         ┌──────────────────┐              ┌──────────────────┐
         │   Unsuitable     │              │  Inappropriate   │
         │    materials     │              │    Activity      │
         └──────────────────┘              └──────────────────┘
                  │                                  │
         ┌──────────────────┐              ┌──────────────────┐
         │   Report to      │              │    Contact       │
         │   eSCo and/or    │              │  Safeguarding/   │
         │   Headteacher    │              │     Child        │
         └──────────────────┘              │   Protection     │
                  │                         │    Service       │
        ┌─────────┴─────────┐               └──────────────────┘
 ┌──────────────────┐ ┌──────────────────┐
 │ If pupil: review │ │ If staff: review │
 │  incident and    │ │  incident and    │
 │   decide on      │ │   decide on      │
 │  appropriate     │ │ appropriate course│
 │ course of action,│ │  of action,      │
 │   applying       │ │  applying        │
 │  sanctions as    │ │  sanctions as    │
 │   necessary      │ │   necessary      │
 └──────────────────┘ └──────────────────┘
                  │
         ┌──────────────────┐
         │     Debrief      │
         └──────────────────┘
                  │
         ┌──────────────────┐
         │     Review       │
         │  policies and    │
         │  technical tools │
         └──────────────────┘
                  │
         ┌──────────────────┐
         │   Implement      │
         │    changes       │
         └──────────────────┘
                  │
         ┌──────────────────┐
         │     Monitor      │
         └──────────────────┘
```

Think then Click
E-Safety Rules for Key Stage 1

These rules help us to stay safe on the Internet

We must have permission from our teacher to use the internet
We only use the internet with an adult

We can   click on the buttons or links when we know what they do

We can   search the Internet with an adult.

We   always ask if we get lost on the Internet.

Think then Click
E-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything, we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We never give out personal information or passwords.
- We never arrange to meet anyone we do not know.
- We do not use Internet chat rooms or social networking sites (e.g., Facebook, Snapchat, Twitter, Instagram or Club Penguin) in school.

E-Safety Rules

These E-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school
- Irresponsible use may result in the loss of network or internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

MOBILE PHONES, CAMERAS AND OTHER ELECTRONIC DEVICES WITH IMAGING AND SHARING CAPABILITIES

Children are not allowed to use personal mobile phones, cameras or other electric devices with imaging and sharing capabilities in school. Children who to need to bring in a mobile phone, for example if they are going home with a different family member, should leave this in the school office and pick up at the end of the day. Staff must ensure that mobile phones and other personal electronic devices with imaging and sharing capabilities are not used for personal use during class time. They will follow the Staff IT Acceptable Use Statement as set out below.

Trust

Friendship   Forgiveness

Kirkoswald C of E School
Website Permission

CONSENT TO ALLOW INTERNET ACCESS & TO TAKE AND USE PHOTOGRAPHS OR OTHER IMAGES OF A CHILD

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to read the e-safety rules on the attached page and to complete the form below confirming their understanding and consent in relation to its use.

We would also like the opportunity to *photograph / film* pupils to help publicise and promote our *school.* We require images to use in leaflets, displays and on the school website. *Please note that websites can be viewed throughout the world and not just in the UK where UK Law applies.*

Images which are subject to the GDPR regulations 2018 and the Data Protection Act 1988 can be viewed upon request and will be used for a maximum of a two-year period before being destroyed. Images that may cause distress or embarrassment to either the child or the parent will NOT be used. **Pupil's names will not be used.**

Please note that in order to comply with the GDPR and Data Protection Act, we also need your consent before we can record or photograph your child, therefore, can you please complete the form below in full noting that consent can be withdrawn at any time.

Name of child (Block Capitals)	
Name of person responsible for the child	

1. Parent's Consent for Internet Access
- I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.
- I understand that the school cannot be held responsible for the content of materials accessed through the Internet.
- I agree that the school is not liable for any damages arising from use of the Internet facilities.

2. Parent's Consent to Take & Use Photographs & Other Images for Publication Electronically & on the Internet
I understand that images being taken of my child will only be used by the school for the following purposes:
- Electronic and printed information, displays and exhibitions publicising the school
- Electronic and printed information, displays and exhibitions relating to the Local Authority / Cumbria County Council
- I understand that the images will NOT be used:
- Where they may be viewed as negative in tone, or may cause offence, embarrassment or distress for the child or parent/carer i.e., drug abuse, child abuse etc.
- In any NEW publication more than two years after the date the original images were taken

Having read the statement above with regard to consent for images / photographs of your child to be taken and used, please tick the appropriate box.

Having read the statement above about consent for images / photographs of your child to be taken and used, please tick the appropriate box.	**YES**, I give consent for pictures to be taken and used
	NO, I do not give consent for pictures to be taken and used
Signature of person responsible for the child:	
Relationship to the child:	
Date	

Please note: There may be other circumstances falling outside the normal day-to-day activities in school, in which pictures of children are requested. The school recognises that in such circumstances specific consent from parents/carers will be required before the school can permit the filming of photography of children.

Staff IT Acceptable Use Statement

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role. During my contracted hours, work that I carry out on computers is directly related to work at Kirkoswald CE School.
- I understand that school information systems may not be used for private purposes (with the exception of my lunchtime) between 9am and 3.30pm.
- I understand that when I am directly involved in the supervision of children on school trips and residential visits my mobile phone is NOT FOR PERSONAL USE. I will ensure, in this situation, that my mobile phone is used solely for the purposes of necessary communication between other staff and myself who are responsible for direct supervision of children's safety and welfare.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission from the Headteacher.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will not have pupils as 'friends' on any social networking site.
- I will not share home/personal e-mail addresses with pupils.
- I will set the highest privacy settings on any social networking site.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

I have read, understood, and agree with the Information Systems Code of Conduct.

Signed:

Capitals:

Date:

Accepted for school:

Capitals:

Date: