E-SAFETY POLICY (INCLUDING ACCEPTABLE USE POLICY/GUIDELINES)

INTRODUCTION

E-Safety encompasses Internet technologies and also electronic communications such as mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences. In addition, it ensures that correct measures are in place to deal with breaches of E-safety.

The safe and effective use of the Internet is an essential life-skill, required by all. However, Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations.

An effective E-safety policy will address these issues and ensure that all staff and students are following the Acceptable Use guidelines. In addition, it will ensure appropriate security measures are in place to protect the school network and filter out inappropriate material.

The school's E-Safety officer is Bob Holderness, who is also the Designated Safeguarding Officer. Issues regarding e-safety, particularly those relating to child safeguarding, should be reported to him.

Our e-Safety Policy has been written by the school, building on the Norfolk e-Safety Policy and government guidance.

It has been agreed by the leadership team and approved by governors.

The E-safety policy and its implementation will be reviewed annually.

Details of legislation surrounding E safety can be found in Appendix 1.

TEACHING AND LEARNING

Why Internet use is important

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. Access to the Internet has been shown to increase motivation and engagement of pupils, particularly those with special or additional needs.

How can we safely use the Internet to enhance learning?

The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Access levels will be reviewed to reflect curriculum requirements and age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and will be given a clear set of rules for using the computers and internet in school (Appendix 3). These rules will be displayed around the school.

Pupils will have clear objectives for Internet use, through planned activities which guide pupils and support the learning outcomes.

Pupils will be taught how to evaluate Internet content

The school will endeavor to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law, including encouraging pupils to acknowledge sources.

Pupils will be taught to be critically aware of the material they read and taught how to validate information before accepting its accuracy

MANAGING INTERNET ACCESS

How will the information system's security be maintained?

The security of the school information system will be reviewed regularly by the ICT Service Engineer, reporting to the ICT co-ordinator and Head of School.

Virus and Spyware protection will be installed and updated regularly.

Security strategies will be discussed with ICT Services, where applicable.

Login details will not be shared.

Passwords to access the administration of the network will be kept by the ICT Service Engineer, Head of School and ICT co-ordinator. Written details of passwords will be kept locked in the safe.

Portable media may not be used by staff to transfer work from home to school in line with school regulations regarding pupil data use. If a member of staff suspects that a home or school device has a device or other problem they must let the IT Technician know as soon as possible and allow the technician access to their portable media for virus scanning.

The ICT Service Engineer will review the system capacity regularly.

How will E-mail be managed?

Pupils may only use approved e-mail accounts in school.

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.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Staff should not contact pupils or parents using personal e mail addresses

Staff should use only their NCC e-mail (GoogleMail) account when dealing with school based issues.

Published content and the school web site

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

The ICT Service Engineer and ICT coordinator will take overall editorial responsibility and ensure that content is up to date, accurate and appropriate.

Photographing pupils and publishing pupil's images and work on the internet

Photographs 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 school website or particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (Appendix 5).

Social networking and personal publishing

The internet access provided by the LA will be set to filter access to inappropriate social networking sites, unless a specific use is approved (eg pupils may have a short period of time where they have access to Facebook, to enable them to learn how to set their privacy settings).

Staff must not access social networking sites for personal use via school information systems or using school equipment.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Staff should not communicate with parents or children using public social networking sites such as Facebook, MySpace, Twitter, etc.

It is inappropriate for pupils of primary age to use Social Network sites.

Managing filtering

The school will work in partnership with the LA and ICT Services to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the ICT Coordinator or the ICT Service Engineer who will then report this site to ICT Services.

MANAGING EMERGING TECHNOLOGIES

Emerging technologies, including technology not used at present in school, will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Other Devices

Children are not permitted to bring ICT devices into school without the permission of the Head of School.

The school allows staff to bring in personal mobile phones and devices for their own use. Staff should not be contacting pupils or parents/carers using their personal devices.

PROTECTING PERSONAL DATA

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

Authorising Internet access

All staff will be directed to read the school E safety policy and will be asked to read and sign the 'Staff code of conduct: Internet and E mail use' (Appendix 2) before using any school ICT resource. In addition all users of school networked computers must agree to the 'Acceptable Use' rules (Appendix 6), which are displayed on screen, before being allowed to log on to any computer.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Parents will be asked to sign and return a consent form.

Pupils and parents must agree to comply with the 'Responsible Internet Use statement' (Appendix 4) before being granted Internet access.

Visitors to the school who require access to a school networked computer will be given restricted access via a 'visitor' log-on.

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 NCC can accept liability for the material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is effective.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Head of School.

Complaints of a child protection nature must be reported to the E safety officer, currently Mr Holderness.

COMMUNICATING THE POLICY

Introducing the E-safety policy to pupils

Safe use of computer rules will be posted in all networked rooms.

Users will be informed that network and Internet use will be monitored.

Instructions in safe and responsible internet use will be given regularly in ICT lessons eg. Using the SMART rules.

Staff and the E-Safety policy

All staff will be shown the School E-Safety Policy, and its importance explained. Staff will be asked to sign the 'Staff code of conduct: Internet and Email use'.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times.

Staff training in safe and responsible use will be provided as necessary.

Enlisting parents' support

Parents'/Carers' attention will be drawn to E-Safety in newsletters and on the website and VLE. All new parents will be asked to sign an E safety agreement when they register their child with the school.

Parents will be invited to attend information evenings where safe home internet use will be discussed.

Evaluation

Evaluation of this policy is carried out primarily by the ICT Co-ordinator, ICT Service Engineer and Head of School. Its effectiveness is regularly reviewed at ICT development meetings.

All staff have a responsibility to adhere to the 'staff code of conduct'; Internet and Email use' and to report any matter of E safety to the appropriate member of staff.

This policy will be reviewed in Autumn 2018

Signed…….Date……

Appendix 1

The Legal Framework surrounding E-safety (01.11.09)

This section is designed to inform users of legal issues relevant to the use of electronic communications. The law is developing rapidly

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

• gain access to computer files or software without permission (for example using someone else's password to access files);
• gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
• impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Freedom of Information Act 2000
The Freedom of Information Act gives you the right to ask any public body for all the information they have on any subject you choose. Unless there's a good reason, the organisation must provide the information within 20 working days. You can also ask for all the personal information they hold on you.
You can ask for any information at all - but some information might be withheld to protect various interests which are allowed for by the Act. If this is case, the public authority must tell you why they have withheld information.
If you ask for information about yourself, then your request will be handled under the Data Protection Act

Education and Inspections Act 2006, sections 90 and 91, provide statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. **Section 94** also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with E-safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

Malicious Communications Act 1988 (section 1) This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Public Order Act 1986 (sections 17 – 29) This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1) It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a

child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from abuse based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003
A new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and then intentionally meet them or travel with intent to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document, which is available from the Home Office website (www.homeoffice.gov.uk/documents/children-safer-fr-sex-crime?view=Binary).

More information about the 2003 Act can be found at www.teachernet.gov.uk

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

APPENDIX 2

Staff Code of Conduct: Internet and Email use.

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 adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head of School or ICT coordinator

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted 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 understand that I am responsible for all activity carried out under my username
- I will ensure that all school generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure email system(s) for any school business
- I will ensure that all data is kept secure and is used appropriately and as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.
- At school, I will not install any hardware or software without the permission of the ICT Service Engineer or ICT coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head teacher.

- I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head of School.

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

Full name:……(printed)

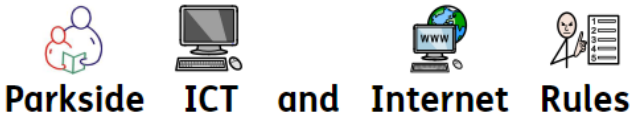
Job title:……

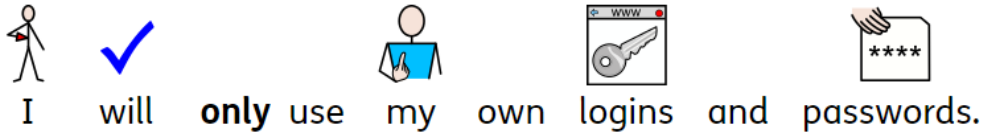
Signature:……**Date:**……

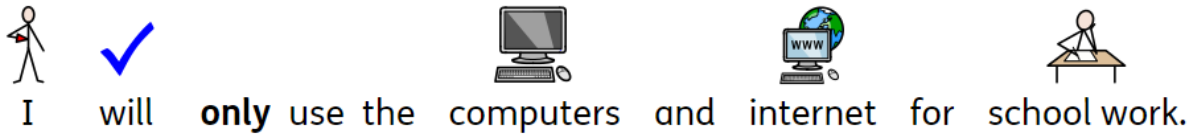
APPENDIX 3

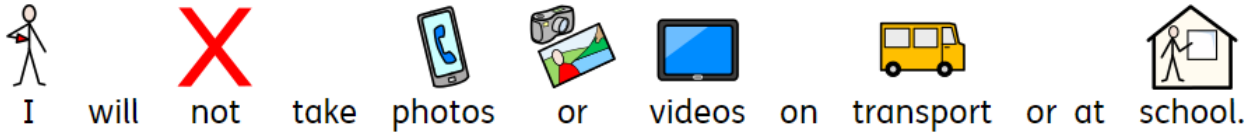
RULES FOR RESPONSIBLE INTERNET USE

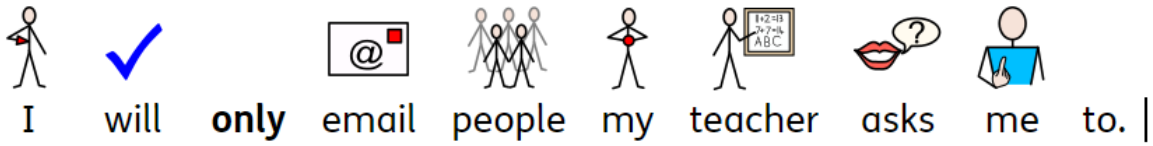
Rules have been updated and are displayed using symbols

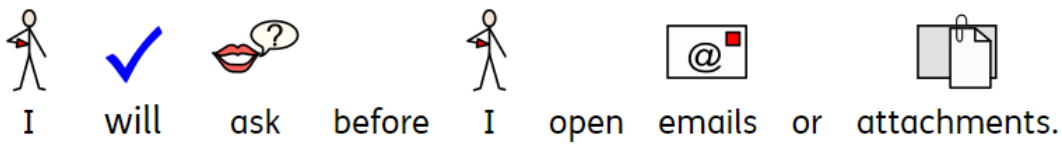


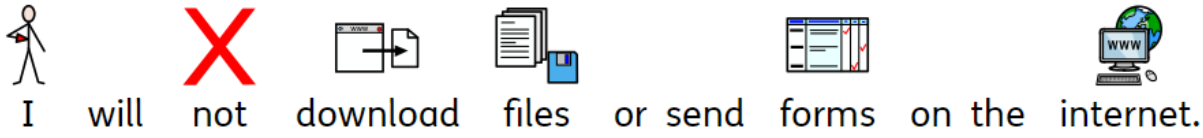


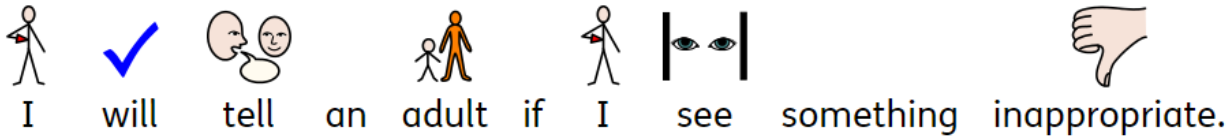


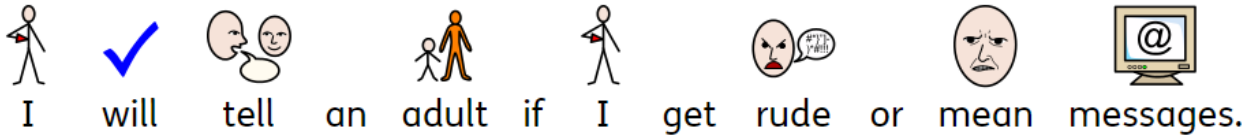


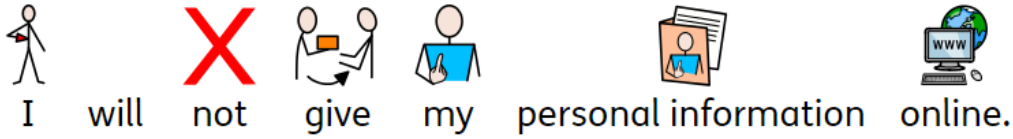


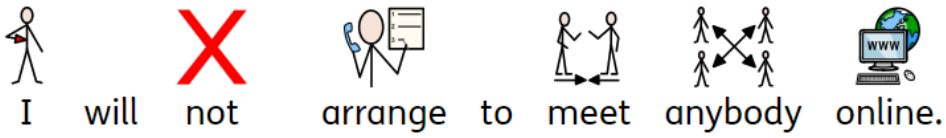












Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our access to the Internet comes through Norfolk's Internet Service Provider project making filtered content available in schools. Children will be introduced to a set of rules and taught how to use the Internet responsibly and safely. When they are given access to the Internet they will be supervised and directed towards specific curriculum activities and suitable web sites. However, the school cannot be held responsible for the nature or content of materials accessed through the Internet.

The school will not be liable for any damages arising from your child's use of the Internet facilities.

The school has prepared an E safety (including acceptable use) policy which is intended to help us make the most of the Internet whilst minimising the risks. It includes a set of Rules for Responsible Internet Use that we will be teaching the children and these can be found overleaf. Should you wish to read the full policy please enquire at the school office. I would ask you to read the enclosed rules with your child and complete the attached permission slip so that your child may use the Internet at school. Please return by……

Should you wish to seek further information regarding Internet use, particularly Internet safety, you may find the following web sites useful:

www.thinkuknow.co.uk
www.childnet.com/kia/parents

If you wish to discuss any aspect of our use of the Internet please telephone me to arrange an appointment.

APPENDIX 5

Consent form regarding use of photographic and video images of children at Parkside School

Dear Parent/ Guardian

Occasionally, we may take photographs and video recordings of the children at Parkside school. We may use these images in our school's prospectus or in other printed publications that we produce, videos of school productions and events, as well as on our website, VLE or on project display boards at our school.
We may also make video or web cam recordings for school-to-school conferences, monitoring or other educational use. Norfolk County Council may also use our photographs of pupils to illustrate work in Norfolk schools in council publications, publicity materials and the Internet.

From time to time the media may visit our school and may take photographs, film footage or carry out radio interviews. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes. Photos for the media and other publicity purposes may also be taken at events where our school is participating.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Please answer questions 1 to 4 below, read the conditions of use attached to this letter and then sign and date the form where shown.

	Please circle your answer
1. May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes or on project display boards?	**Yes / No**
2. May we use your child's image on our school website and VLE?	**Yes / No**
3. May we record your child's image on video or webcam?	**Yes / No**
4. Are you happy for your child to appear in the media? (Please be aware that the press may use full names with photographs)	**Yes / No**

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

The conditions for use of these photographs/images are attached.

I have read and understood the conditions of use.

Child's name…….

Parent / guardians name ……. (Please print in block capitals)

Parent / guardian signature……

Relationship to child…….. Date…….

Conditions of use

1. This form is valid for the period of time your child attends this school, plus one year after they leave. The consent will automatically expire after this time.

2. We will not re-use any photographs or recordings for more than one year after your child leaves this school.

3. We will not use the personal details or full names (which means first name **and** surname) of any child in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.

4. We will not include personal e-mail or postal addresses, telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

5. We may include pictures of pupils and teachers that have been drawn by the pupils.

6. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".

7. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

8. **Please note** that the press are exempt from the Data Protection Act and may want to include the names and personal details of children and adults in the media.

9. **Please note**, the Data Protection Act is not relevant for parents who wish to take photos or record an event for their own personal use. Parents are not permitted however, to take photographs or make a recording for anything other than their own personal use. To do so would require consent of other parents whose children may be captured on film and if this was not given would mean parents concerned would be in breach of the Data Protection Act.

10. Please carefully consider before posting photographs of your child on social media particularly if they are wearing their school uniform. **It is not permitted** to post any photographs or videos which contain the image of another child. To do so you must have the consent of the other child's parents.