E-Safety (Prep School) Policy

Ref: ***LP-PP-012***	Version: **5.7**	Date: *18th August 2020*
Document Owner: Helen Roe ***(ICT Subject Coordinator)***		
Description: This policy outlines the Prep School's approach to e-safety.		

OUR SCHOOL AIMS

- *To foster intellectual curiosity and a love of learning.*
- *To achieve high academic standards in a supportive but disciplined atmosphere.*
- *To equip pupils with the skills and knowledge to meet the challenges of our rapidly changing world.*
- *To instill an enthusiasm in interests and opportunities beyond the classroom.*
- *To support pupils' development of a sense of justice and an awareness of their rights and responsibilities as global citizens.*

1.0 INTRODUCTION

1.1 The school recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

1.2 E-safety can be described as the school's ability to:

- Protect and educate pupils and staff in their use of technology.
- Have the appropriate mechanisms to intervene and support any incident where appropriate.

1.3 The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material.
- **Contact:** being subjected to harmful online interaction with other users.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

(Ofsted – Inspecting e-safety in schools)

1.4 In order to help our pupils to better understand these areas of risk, the Prep School has adopted the acronym SMART. This stands for Safe, Meeting, Accepting, Reliable and Tell.

1.5 The e-Safety Policy is part of the School Development Plan and relates to other policies including those focused on cyberbullying, anti-bullying, behaviour management and for child protection. Please see other policies connected with e-Safety listed at the end of this document.

1.6 The Prep School's e-Safety Co-ordinator is the Head of Prep School, who is also the Designated Safeguarding Lead.

1.7 This e-Safety Policy has been written, building on best practice and government guidance. It has been agreed by Senior Management and approved by Governors. The Policy and its implementation is reviewed annually.

2.0 TEACHING AND LEARNING

2.1 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. However, the benefits of internet access are tempered by its inherent risks, and the school is of course aware that all of its members, whether staff, parents or pupils, rely increasingly heavily on the digital world. It is a valuable tool for teaching and research, but the rules to infringe abuse need to be stringent and frequently reviewed.

2.2 It is recognised that keeping safe on-line is as much about educating pupils to think critically and about appropriate behaviour on-line as technical solutions. Staff are aware that some children may be more vulnerable to risk from internet use, generally those children with a high level of computer skills, coupled with poor social skills.

2.3 The below details our approach on the use of the internet in school:

- The internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. E-safety is taught as part of the Computing & PSHECE programme in an age-appropriate way. This is addressed each year as pupils become more mature, and the nature of newer risks is identified. A staff e-safety guide with objectives and resources for each year group is kept in the computing folder on Prep Staff common under e-safety.
- The school SMART rules (detailed in the section below) are taught explicitly to Year 1 and Year 3 and reinforced and referred to in other year groups. The e-safety curriculum underpins the e-safety SMART agreement that pupils and their parents/carers are required to sign at the start of each academic year
- Pupils are educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils are also shown how to publish and present information appropriately to a wider audience, and to be critically aware of the materials they read before accepting its accuracy.
- Pupils and parents/carers in Years 5 and 6 attend Internet Safety Workshops biannually and then again in the Senior School.
- Pupils in Key Stage 2 are taught how to report unpleasant internet content to the teacher.
- The school's Acceptable Use of Computers Policy is given in full at the point of log-on for every student and member of staff (please see **Appendix A:** *Acceptable use of Computers Policy*).
- The school's internet access is provided by Zen Internet, which includes filtering appropriate to the age of pupils. However we are aware that this may not be the same for children at home and that education about how to stay safe is crucial.
- The school seeks to ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.

Key e-safety messages:

Children need to be guided on:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies then can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that they won't be blamed if they report any e-safety incidents
- that cyberbullying cannot be tolerated
- the basic principles of how to behave on the internet

3.0 SMART E-SAFETY RULES

3.1 Every year children and their parents/carers are required to sign an e-safety SMART agreement. This is linked to the SMART acronym (Safe, Meeting, Accepting, Reliable and Tell). This set of rules are taught explicitly at the start of Year 1 and Year 3. They are reinforced and referred to in Computing lessons in all other year groups and are built upon as the maturity of the children develop.

3.2 The display in the main computing room shows the e-safety rules and agreements. These rules are also on display next to any computers in classrooms that children have access to. All computers accessed by the children have a 'Remember SMART' sticker attached to them.

Rules for KS1

S I will stay **SAFE** by not putting any of my details on the internet, like my phone number or address.

M I will not **MEET** anyone online I don't know in real life.

A I will not **ACCEPT** and open emails and messages from people I don't know.

R I understand that information I find on the internet may not be **RELIABLE** or true. I will check by asking an adult.

T I will **TELL** my teacher or parent if something online makes me feel uncomfortable or worried, or if someone I know is being bullied online. If I see something on screen that I am unhappy with I will turn off or minimise the screen and tell a teacher.

Rules for KS2

S I will stay **SAFE** by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M **MEET**ing someone you have only been in touch with online can be dangerous. I will not **MEET** anyone I've met online in real life. Remember, online friends are still strangers even if you have been talking to them for a long time.

A I will not **ACCEPT** and open emails, attachments or IM messages from people I don't know or trust. I know that these can contain viruses or nasty messages.

R I understand that information I find out on the internet may not be **RELIABLE** or true. I will check information by looking at other websites, in books, or with someone who knows. I also understand that someone I speak to over the internet may be lying about who they are.

T I will **TELL** my teacher or parent if something online makes me feel uncomfortable or worried, or if someone I know is being bullied online. If I see something on screen that I am unhappy with I will turn off or minimise the screen and tell a teacher.

3.3 Other rules: (applicable to both key stages)

- The messages I send will always be polite and sensible.
- I will only use the computers/iPADs with permission and as instructed by the teacher.
- I will keep my computer user name and password secret. My teacher will keep a list of my computer user name and password if I forget them.
- I will not upload photographs of myself and/or my friends which have been taken in school or whilst we are in school uniform onto social media sites.

3.4 Most situations we experience in the Prep School are encompassed under the rules above, however there are some more explicit statements which can be found in the School Behaviour Management Policy and School Rules and these rules form part of the e-safety agreement that children in KS2 sign. They are as follows:

- Pupils must not interfere with the work of others or the system itself.
- No one must create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person.
- Pupils must not gain or attempt to gain unauthorised access to other people's files or facilities or services accessible via local or national networks or transmit any confidential information about the School: they must not attempt to get around service limitations placed on network use by the School (or its agents).
- Pupils must not use school computers to access any social networking sites.
- Pupils must not under any circumstances use any social networking sites e.g Facebook or Twitter in order to bully or intimidate any pupil or member of staff or behave in any way online which could bring the school into disrepute.

4.0 SCHOOL SYSTEMS

4.1 The school system security is maintained and monitored daily by the ICT Engineers. The School uses iboss to filter and monitor inappropriate content. The filtering is based on a category system, and there are blocks on the categories that are deemed inappropriate for school use. In line with government advice and the Prevent Strategy, these blocks include categories regarding terrorist and extremist material.All web traffic is logged and monitored. If the content is on the blocked list, an 'access denied' page is displayed. If something inappropriate is accessed on the school computers it must be reported immediately by a member of staff to the ICT Engineers who will then review the usage log and block the inappropriate conduct. Every day, the Deputy Head (Pastoral) is sent a log of any searches made by staff or pupils that has been blocked, and where relevant pupils and parents have been contacted to discuss the nature of such searches.

4.2 The school system is protected by an anti-virus system which scans all files on access, both which are stored on our system and also those on USB pens. Emails are scanned when they are received for inappropriate language, spam and dangerous attachments. Spam and emails with inappropriate language are blocked and dangerous attachments are stripped from emails. The ICT Engineers regularly monitor the quarantined mailbox, and anything that has gone in here unnecessarily can be released.

MANAGING INTERNET ACCESS

5.0 INFORMATION SYSTEM SECURITY

5.1 All members of staff have their own personal username and password which should be kept private. When staff leave the school this username and password is deleted. Computers in school log out after a short period of inactivity to prevent access from unwanted people. Children are not allowed into classrooms unsupervised or without permission. Children are not allowed to use school computers without permission.

5.2 Staff accessing iSAMS, VMWare and school systems at home take responsibility for ensuring they are using a secure computer. Computers logged into school systems should not be left unattended and when staff have finished working they must log out of all school systems to prevent unwanted access. Staff are encouraged to use the school system to access files at home rather than carry data on memory sticks which can become lost.

- Staff are expected to change their passwords every 90 days, The last 3 passwords cannot be used, Must be minimum of 8 characters, which must include, uppercase character, lowercase character, and a number.
- School ICT systems security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the internet provider & Rivanet.
- ISAMS, the school's information system, is cloud based and backed up externally by iSAMS.

6.0 PROTECTING PERSONAL DATA

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

7.0 AUTHORISING INTERNET ACCESS

7.1 All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

7.2 The school maintains a current record of all staff and pupils who are granted access to school ICT systems

7.3 Pupils apply for internet access individually by agreeing to comply with the Responsible Internet Use statement when they log on to any school computer or device.

8.0 ASSESSING RISKS

8.1 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. The school cannot accept liability for the material accessed, or any consequences of internet access.

8.2 The school monitors ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

9.0 MANAGING FILTERING

9.1 If staff or pupils come across unsuitable on-line materials, the site must be reported to the Designated Safeguarding Leader (J. Shackel) and to ICT.

9.2 Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Staff check any website they wish to use with pupils for appropriate content. This will be done before the lesson takes place.

10.0 MANAGING EMERGING TECHNOLOGIES

10.1 Emerging technologies will be examined for educational benefit.

10.2 Mobile phones and associated cameras are not be used during lessons or formal school time. Pupils are only allowed phones in school in exceptional circumstances and with permission from the Head of Prep School.

10.3 The appropriate use ofFirefly, laptops and alternative learning platforms is discussed as the technology and resources become available within the school. Pupils from Years 1 to 6 may use Firefly and Teams, especially when remote learning. Pupils in Nursery or Reception will use ILD (Interactive Learning Diary).

10.4 Staff use of mobile devices is restricted during the school day when they are around pupils, and reference is made to this in both the Staff Code of Conduct and the Safe Working Practice forms. It is not permissible for any adults to use mobile phones in the EYFS. All personal mobile phones must be locked away upon entering the building.

10.5 Staff will use a school phone where contact with parents is required, unless necessary on school excursions or sporting fixtures.

11.0 PUBLISHED CONTENT AND THE SCHOOL WEBSITE

11.1 The contact details on the website are the school address, email and telephone number. Staff or pupils' personal contact information is not published.

11.2 The Headmaster or nominees take overall editorial responsibility and ensures that content is accurate and appropriate.

12.0 E-SAFETY TRAINING FOR STAFF

12.1 It is important that all staff are aware of the risks online activity poses to children. They must be aware that this risk includes the danger of children being exposed to extremist and terrorist material online. Prevent awareness training is being rolled out across the school.

12.2 The Designated Safeguarding Leader (DSL – J Shackel) will be responsible for keeping staff up to date via the following:

- Staff meetings, which provide a weekly forum for updates.
- An E-Safety Trainer will specifically train class teachers in e-safety every two years, and staff in Upper Key Stage Two will also be part of the e-safety lessons given to the children by an external trainer.
- **Keeping Children Safe in Education** (statutory guidance for schools and colleges April 2014) will be distributed to all staff and there will be whole staff child protection inset days every three years and new staff will receive training on child protection within 3 months of starting or during induction.

13.0 CHILD USER ACCOUNTS

13.1 All children from year 1 – 6 are issued their own username and password for access to the school computers. Years 1 to 3 will mainly only require this if doing remote learning. They will also have a username and password for any learning platforms that they may use eg. Firefly, Microsoft Teams, Purple Mash, Moodle, Google apps. Children are taught the importance of keeping their log in details secret and not sharing them unnecessarily to help them develop good habits from an early age. KS1, Reception and nursery age children will use a class log in.

13.2 Children's work in years 1-4 is saved in year group folders and thus accessible to other children. Children are taught to respect each other's work and are not permitted to access other children's files without their permission. Children in Year 5 and 6 save their work to their individual account to which only they and their class teacher can access.

14.0 E-MAIL

14.1 Pupils in all Years are given a school email address so they can access remote learning during the COVID-19 pandemic. They are taught how to use email in a safe way including how to deal with junk mail and email from unauthorised senders.

When using email, students are taught:

- to keep messages polite.
- not to disclose personal contact details for themselves or others.
- to tell their parent, carer or teacher immediately if they receive an offensive or distressing email.
- not to use email to bully or harass others.
- to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

14.2 From KS2 suitable forms of email communication are regularly explained to pupils in accordance with the guidelines set out by the information and Records Management Society (www.irms.org.uk)

14.3 SMART posters are displayed in all rooms where computers are used.

14.4 Pupils must immediately tell a teacher if they receive an offensive e-mail or Teams message.

14.5 Pupils are advised not to reveal personal details about themselves or others in e-mail communication or Teams message, or arrange to meet anyone without specific permission.

14.6 Staff to pupil communication can take place via email or Teams. Emails must take place via a school email address or from within Firefly, and will be monitored. Teams can be used for communication but must only be used during school hours (8am-5pm), this is monitored.

14.7 Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

14.8 The forwarding of chain letters is not permitted.

15.0 USE OF CAMERAS, MOBILE PHONES, PUBLISHING CHILDREN'S DETAILS/PHOTOGRAPHS ONTO THE SCHOOL WEBSITE

*See Use of Photographs Policy and Child Protection & Safeguarding Policy

16.0 PUBLISHING PUPILS' IMAGES AND WORK

16.1 Photographs that include pupils are selected carefully and will not enable individual pupils to be clearly identified. Wherever possible, the school will seek to use group photographs rather than full-face photos of individual children.

16.2 Pupils' full names are avoided on the website, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

16.3 Written permission from parents or carers is obtained before photographs of pupils are published on the school website.

16.4 Parents are clearly informed of the school policy on image taking and publishing on the school website.

17.0 CYBERBULLYING

17.1 Cyberbullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike traditional physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

17.2 Cyberbullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. In extreme cases, cyberbullying could be a criminal offence.

17.3 Cyberbullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing videos of someone via mobile phone or email

17.4 Most incidents of cyberbullying will not necessarily reach significant harm thresholds and will probably be best dealt with the service's own anti-bullying or acceptable use policies with the co-operation of parents.

17.5 In terms of Cyberbullying, students are taught:

- not to disclose their password to anyone
- to only give out mobile phone numbers and email addresses to people they trust
- to only allow close friends whom they trust to have access to their social networking page
- not to respond to offensive messages
- to tell a responsible adult about any incidents immediately.

18.0 HANDLING E-SAFETY COMPLAINTS & CONCERNS

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

18.2 Any complaint about staff misuse must be referred to the Headmaster.

18.3 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

18.4 Pupils and parents are made aware of the complaints procedure.

18.5 Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and breaking the SMART rules and this will be in line with the school's Behaviour Management Policy.

18.6 All use of the school internet connection by community and other organisations is in accordance with the school e-safety policy.

18.7 Parents and carers are advised to be vigilant about possible cyberbullying and how to work with internet and mobile service providers to cut down on the risk of cyberbullying:

- mobile phone companies can trace calls and ensure that any further calls and texts from that number are blocked

- internet service providers can trace messages being sent from a personal email account and can block further emails from the sender
- where bullying takes place in chat rooms, the child should leave the chat room immediately and seek advice from parents; bullying should be reported to any chat room moderator to take action
- website providers can remove comments from social networking sites and blogs and in extreme cases, can block the bully's access to the site
- the child could change mobile phone numbers or email addresses.

19.0 INAPPROPRIATE CONTACTS AND NON-CONTACT SEXUAL ABUSE

19.1 Children may also be sexually abused online through video messaging such as Skype. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records them. The perpetrators may be adults but may also be peers.

19.2 Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. If reported to the school, students and parents are advised on how to terminate the contact and change contact details where necessary to ensure no further contact. Parents are advised to be vigilant of their child's internet use and report any concerns or incidents.

19.3 In the event of such an incident, the child should be taught how to use the CEOP "Report abuse" button (normally displayed on the screen) and parents should contact the police to report the incident.

19.4 Staff and parents should contact Surrey Children's Services on (0300) 123 1620 (or if outside working hours, the emergency duty team on (01483) 517898) for advice on making a referral where there are concerns that the child:

- is being groomed for sexual abuse
- is planning or has arranged to meet with someone they have met on-line
- has already been involved in making or viewing abusive images
- has been the victim of non-contact sexual abuse.

19.5 If staff or parents are aware that a child is about to meet an adult they have made contact with on the internet, they should contact the police on 999 immediately.

20.0 ONLINE CHILD SEXUAL EXPLOITATION (CSE)

20.1 CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not aware that they are being abused.

20.2 Staff should be aware that children can be sexually exploited online, for example posting explicit images of themselves in exchange for money or goods.

20.3 If staff are concerned that a child they work with is being sexually exploited online, they should inform the Designated Safeguarding Lead immediately, who may make a multi-agency referral.

21.0 WEBSITES ADVOCATING EXTREME OR DANGEROUS BEHAVIOURS

21.1 Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

21.2 Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

21.3 Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

21.4 Where staff are aware that a young person is accessing such websites and that this is putting them at risk of harm, they should consider making a referral to Surrey Children's Services.

22.0 STAFF AND THE E-SAFETY POLICY

All staff are given the School e-Safety Policy and its importance explained.

- All staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.
- Staff are made aware in the Staff Code of Conduct that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use are supervised by senior management in the Senior School and have clear procedures for reporting issues.

23.0 ENLISTING PARENTS' SUPPORT

23.1 Parents and carers have access to the e-Safety Policy on the school website.

23.2 The school will ask all new parents to sign the SMART agreement when they register their child with the school, and every existing pupil will be expected to sign the agreement every year.

23.3 The school is looking into ways in which parents can be given e-safety training with a focus on education and being given an overview of the means by which they can take control whilst not undermining trust.

23.4 Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel, interaction and exploration. Parents should be encouraged, where appropriate, to interact with their children on the internet as well as provide other opportunities for recreation.

23.5 Homework tasks may be uploaded to Firefly, therefore parents may wish to check this to see status.

24.0 OTHER POLICIES AND DOCUMENTS LINKED TO THIS E-SAFETY POLICY:

24.1 Policies

- Anti-bullying Policy & Cyberbullying
- Behaviour Management Policy
- Complaints

- Use of ICT Policy
- Child protection & Safeguarding Policy
- Staff Code of Conduct

Data Protection

- Digital Images
- Use of Photographs
- Whistleblowing
- Exclusion
- SEND
- Internet and Social Networking Policy (Staff)
- Lingfield College Computer Usage Policy
- See School Rules

24.2 Documents

- The Data Protection Act (1988)
- The Computer Misuse Act (1990)
  - Unauthorised access (e.g. using another user's username and password)
  - “hacking”, “introduction of viruses”
  - Unauthorised modification of the contents of a computer (installing software in your account)
- The Copyright, Designs and Patents Act (1988)
- Copyright (computer programs) regulations (1992)

  It is an offence to:

  - Copy software unless allowed by license
  - Download copyright materials (which may include MP3's)
  - Link to a site that contains material used without permission
- Public Interest Disclosure Act (1998)
- Obscene Publications Act (1959)
  - It is an offence to sell, hire or lend material that is obscene
  - This includes publishing or downloading pornographic or other offensive material from the web
- Telecommunications Act (1984)
  - It is an offence to transmit messages over telecommunications systems (including computer networks) of an obscene, slanderous, threatening or annoying nature
  - This INCLUDES the contents of e-mail

- Theft Act (1968)

  The following acts are ILLEGAL:

  - Hacking
  - Intentional introduction of viruses
  - Giving someone unauthorised access (which includes giving away your password): It is NOT your account to lend to others. Actions of another whilst using your account are YOUR responsibility.
  - Downloading/storing material that is obscene
  - Downloading illegal copies of software
  - Sending messages of an obscene, slanderous, threatening nature
  - Installation of unlicensed software

24.3 These explanations are intended to be a guide as to how the acts relate to your use of the computing or network facilities and are not a legal interpretation of those acts.

25.0 DISCIPLINARY ACTIONS

Depending on the severity of the offence, either one or two or all of the following actions taken could be:

- Informal Warning given in school.
- Letter sent home (recorded in pupil's file).
- Withdrawal of ALL parts of user account.

26.0 DAMAGE TO EQUIPMENT:

The following Damage to Equipment policy statement will be published:

- Any purposeful or wilful damage (be this at a physical or software level) to or theft of equipment will be charged for at the current rate. Theft of equipment of any kind takes money away from that available to improve facilities within the school.
- It is in your own interest, and the interest of other pupils within the school, that the computer equipment is treated with utmost respect.
- Damage to or theft of equipment will cause inconvenience to you and to others.

Last reviewed August 2020

Next review due August 2021

Appendix A

Use of Digital Images (Photography & Video)

Dear Parents,

At Lingfield, we take photographs or videos of our students when they are involved in school activities. There are many opportunities for digital imagery to be used, e.g. during a learning activity to demonstrate or evaluate work, to give presentations, to share good practice with the wider community or to celebrate achievements.

These images may be displayed on our website or Twitter feed, which is public-facing and could potentially be viewed by anyone on the internet, or they may be displayed on Firefly, our VLE (Virtual Learning Environment), which is private to the school community and can only be viewed by those with a username and password. Occasionally, the school may be visited by the news media (usually local newspapers) to take photographs or film of an event at the school. Pupils will often appear in these images which will be published in local newspapers or broadcast on television.

To comply with the Data Protection Act 1998, we need permission to use photographs or recordings of any child, and observe the following regulations:

- When posting images for external use, we avoid using surnames
- If showcasing digital video work to an external audience, we take care to ensure that pupils are not referred to by name on the video, and that pupils' full names are not given in credits at the end of the film
- Only images of pupils in suitable dress will be used

We would like to ask your permission for the use of digital images. Please answer the following questions and return the form to the School Office:

1. May we take photographs of your child and use them (unidentified by their full name) in publications, on the school website and on video or webcam?

    Please circle your answer: **YES / NO**

2. Do you consent to your child being photographed by local newspapers and other news media on the basis that their full names may be published along with the picture?

    Please circle your answer: **YES / NO**

I have read and understood this document. I understand that images of my child(ren) will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Name of Pupil(s): ________________________________ Form: ____________

Signed: __________________________ (Parent/Guardian) Date: _____________

Please return this form to the School Office.