E-Safety Policy

This Policy was reviewed by the ICT Co-ordinator

May 2023

Next review date May 2024

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing (e.g blogs). It highlights the need to educate pupils, staff and parents about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to use this technology safely. This policy also raises the profile of E-Safety so that all the staff, including Governors, recognizes E-Safety as an issue that is the responsibility of all.

The school's E-Safety policy will operate in conjunction with other policies including those for Anti-Bullying, Curriculum, Data Protection and Child Protection.

This E-Safety policy provides a school E-Safety policy that has been guided and approved by the Children, Families and Education Directorate (CFE).

End to End E-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible Computing use by all staff and students; 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.

Management of Digital Safeguarding

Clearly stated roles and responsibilities-

- **Governors**

Governors are responsible for the approval of the Digital Safeguarding and E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Curriculum Committee receiving regular information about online safety incidents and monitoring reports.

- **Headteacher**

The headteacher will ensure that the digital safeguarding/E-safety policy is implemented and will monitor compliance with the policy, and that appropriate roles and responsibilities of the school's digital safeguarding structure is in place. They will ensure regular reports on the monitoring outcomes for digital safeguarding are reported to the governing body.

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-safety Co-ordinator.
- The Headteacher and DSL/DDSLs should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

• **Nominated e-safety co-ordinator**

There is an identified e-safety co-ordinator (Computing lead) who is responsible for e-safety developments in school and sharing of practise with staff and the wider community of governors and parents.
This person will be in receipt of current training of the latest guidance and procedures and is the main contact for local authority e-safety networks.

• **Network Manager / Technical staff:**

The Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and E-Safety Safety Coordinator for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies

• E-safety governor

There is an identified safeguarding governor who monitors and liaises with the e-safety co-ordinator and who will report to the full governing board.

• E-safety responsibility within subject and management roles

All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility, deputising to any of the above roles where necessary.

• Teacher

All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. They need to work to the agreed guidelines. They have a "front line" monitoring and reporting role for incidents.

- they have an up to date awareness of online safety matters and of the current school Digital Safeguarding and E-Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher, DSL
- all digital communications with pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities

- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

• Learning Mentor

The learning mentor will work alongside the e-safety co-ordinator to monitor e-safety incidents within school and help to deliver appropriate education to children and parents who are involved.

• Support Staff

As for teaching staff, however, given the nature of their role, learners may find it easier to disclose incidents to them. Support staff should be clear about the reporting procedures and use these when incidents occur.

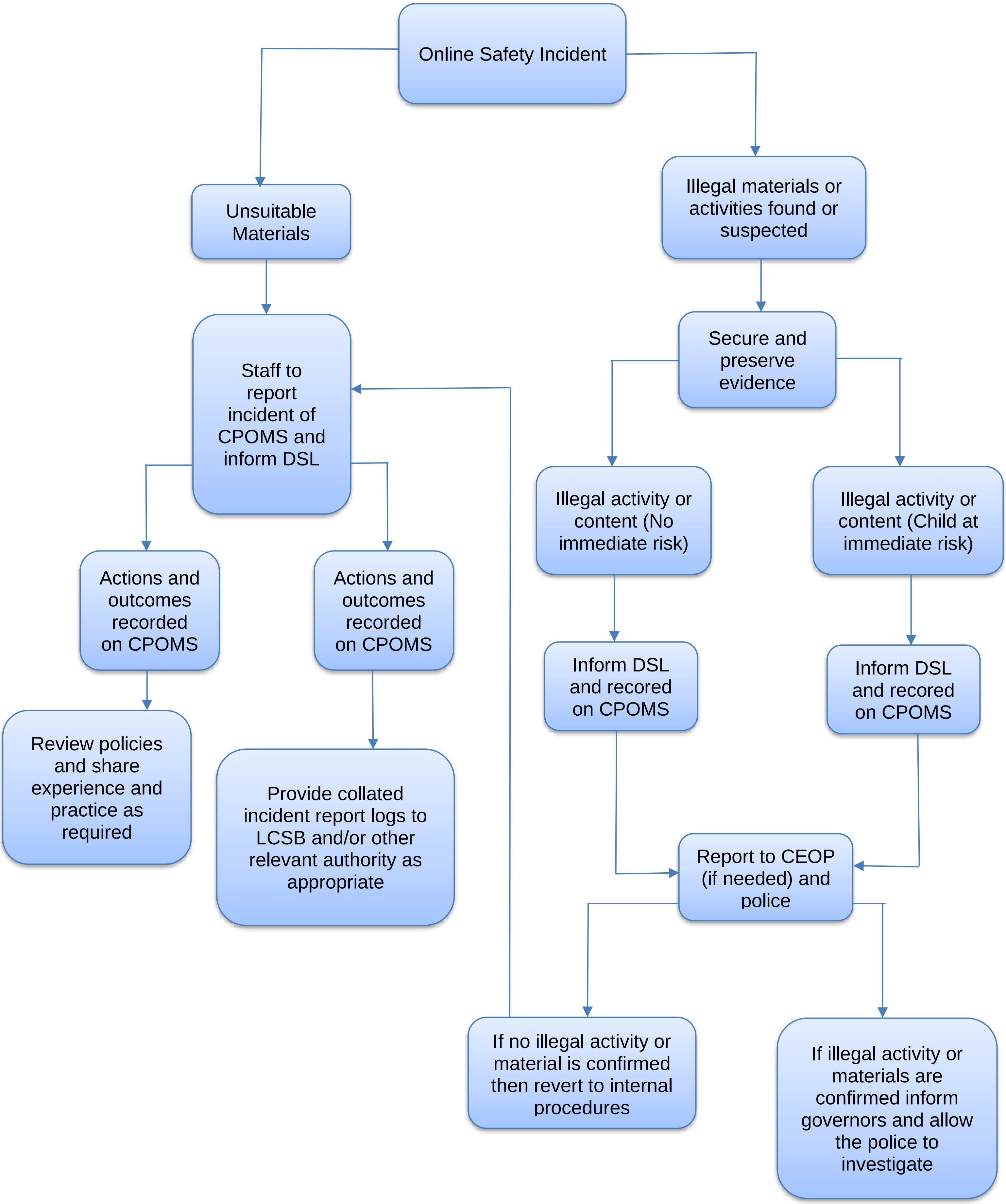
• **School Council Representatives and Digital Leaders**

As a responsible member of their class, the school council need to have e-safety as an item on their agenda. These representatives could help to monitor the appropriate use of technology at a learner level within the school.

Procedures

- All staff and members of the school workforce and children will sign an AUP (acceptable use policy) on an annual basis to ensure that all changes have been agreed.
- Children will be taught about the CEOP report abuse button during e-safety lessons. E-safety issues should be reported to class teacher or e-safety co-ordinator.
- A log of e-safety incidents will be kept on the CPOMS behaviour tracker and these will be reviewed termly by the DSL to ensure that next steps have been implemented.
- If child safeguarding issues arise they will be reported to the safeguarding co-ordinator and procedures as defined in the school’s safeguarding policy will be followed.
- If necessary the headteacher and safeguarding co-ordinator will follow appropriate procedures for reporting incidents beyond the school to the LA.
- All staff are entitled to training and support regarding e-safety. This will be delivered on a regular basis and a record of its delivery will be kept.
- E-safety education is built into our RHE and computing curriculum with e-safety education being delivered at an appropriate level on a regular basis. Our e-safety curriculum map outlines objectives taught each year.
- We will endeavour to provide appropriate training for parents and keep a log of training provided.

- E-safety teaching will be monitored as part of our teaching and learning policy.
- The incident log will be reviewed to effectively assess the impact of e-safety practise and this will be used to inform future planning.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Staff to report incident of CPOMS and inform DSL
Secure and preserve evidence
Actions and outcomes recorded on CPOMS
Actions and outcomes recorded on CPOMS
Illegal activity or content (No immediate risk)
Illegal activity or content (Child at immediate risk)
Inform DSL and recored on CPOMS
Inform DSL and recored on CPOMS
Review policies and share experience and practice as required
Provide collated incident report logs to LCSB and/or other relevant authority as appropriate
Report to CEOP (if needed) and police
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed inform governors and allow the police to investigate

1.1 Writing and reviewing the E-Safety policy

The E-Safety policy is part of the school improvement plan and relates to other policies including those for computing, anti-bullying and for child protection.

- The school has appointed an E-Safety leader. This role is shared by the designated safe guarding lead and the Computing leader.
- Our E-Safety policy has been written by the school, building on the NSPCC Child protection, safety and security E-Safety guidelines. It has been agreed by Leadership Team, E-Safety leaders and approved by governors.
- The E-Safety policy and its implementation will be reviewed annually using the audit in appendix 2.
- The E-Safety policy was revised by: Ian Widdowson (E-Safety leader)

1.2 Teaching and learning

1.2.1 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2.2 Internet use will enhance learning

- 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.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

1.2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 Managing Internet Access

1.3.1 Information system security

- School Computing systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Capacity 2 Learn.

1.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- The forwarding of chain letters is not permitted.
- Incidents of ‘Cyber-bullying’ through e-mails should be passed on to the Head teacher.
- Staff should use school email addresses for school business.
- Staff should not open or download file attachments unless they are certain of their content and origin.

1.3.3 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 pupils’ personal information will not be published.
- The head teacher and business manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupil’s images and work

- Photographs that include pupils will be selected carefully.
- Pupils’ full names will not be used on the Website in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Work published on the Website will be carefully selected in order to encourage anonymity.

1.3.5 Use of Twitter, other social networking and personal publishing

- The school will block/filter access to social networking sites.
- 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.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils and parents will be advised on how to access and use the privacy settings on social media platforms.

- The school will take action if any of the following actions are committed by pupils or staff.

    - ❖ Offensive language aimed the staff, school, parents, governors or others affiliated with the school.
    - ❖ Unsuitable comments or pictures posted on feeds.
    - ❖ Images or text which infringe upon copyright.
    - ❖ Comments that aim to undermine the school, staff, parents, governors or others affiliated with the school.

1.3.6 Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader.
- The E-Safety Leader and technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.8 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 allowed in school time and must be handed to the office for safe-keeping. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

1.4 Policy Decisions

1.4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable Computing Use Agreement' before using any school Computing resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form (appendix 3).

1.4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. 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. Neither the school nor Leicester City Education Authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit Computing provision to establish if the E-Safety policy is adequate and that its implementation is effective.

1.4.3 Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by the head teacher.
- Any complaint about staff misuse must be referred to the head teacher or governing body.
- Complaints of a child protection nature must be dealt with in accordance with Folville's Child Protection procedures.

1.5 Communications Policy

1.5.1 Introducing the E-Safety policy to pupils

- E-Safety rules will be posted in appropriate rooms and discussed with the pupils at the start of each academic year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be taught about E-Safety through specific units of work which form part of the Computing rolling programme.

1.5.2 Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will receive accredited E-Safety training.

1.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Web site.
- Parents will be made aware of that they can contact the E-Safety Co-ordinator at: E-Safety @folville.leicester.sch.uk

Appendix 1: E-Safety - Possible teaching and learning activities

Activities	**Key E-Safety issues**	**Relevant websites/Apps**
Learning about cyberbullying	Pupils should be supervised. Relevant material should be used.	NSPCC THINK U KNOW Anti-Bullying Alliance
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught how search engines work. Integral to this is pupils fully understanding the procedure to follow should they come across any inappropriate material: screen off and hands up.	Web quests e.g. Google
Creating an Advert	Parental consent should be sought. Pupils should seek staff and pupils permission before filming them Pupils be taught about copyright	IMovie
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication for websites other than school. Pupils' full names and other personal information should be omitted.	Folville Junior Website
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name.	Folville Junior Website

Appendix 2: E-Safety Audit

This quick audit will help editing and rewriting the policy annually.

Has the school an E-Safety policy that complies with CFE guidance?	Y/N
Date of latest update:	
The policy was agreed by governors on:	
The policy is available for staff at:	
And for parents at:	
The Designated Child Protection Leader is:	
The E-Safety Leader is:	
Has E-Safety training been provided for both students and staff?	Y/N
Do all staff sign an Computing code of conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the school E-Safety rules?	Y/N
Have school E-Safety rules been set for students?	Y/N
Are these rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y/N
Has an Computing security audit has been initiated by Leadership Team, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Appendix 3: Responsible Computing Use

RESPONSIBLE COMPUTING USE

Name of Pupil Class

We use the school computers and internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

Pupil's Agreement

1. On the network, I will use only authorised log-in names and passwords, which I will keep secret.
2. If I see anything I am unhappy with, or I receive a message I do not like, I will tell the Teacher immediately.
3. I know that the School may check my computer files and may monitor the internet sites I visit.
4. I will look after the Computing equipment that I use.
5. I will not take part in any on-line internet chat groups.
6. I will only use the internet while supervised by a member of staff.
7. I will only use web sites as guided by my Teacher.
8. I will only use E-mail as instructed by my Teacher (all E-mail use at Folville is internal).
9. I will only send non-offensive and sensible E-mails.
10. I understand that my E-mails may be monitored.
11. I will not give any information on the internet, such as name, home or school address, telephone number and personal E-mail.
12. I understand and agree to follow the above.

Signature of pupil:
Date:

Parent's Consent for Internet Access

I have read and understand the school rules for responsible Computing and Internet use and give permission for my child (named above) to access the Internet. I understand that the School will take all reasonable
Pre-cautions to ensure pupils cannot access inappropriate materials.
I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet.
I agree that the School is not liable for any damages arising from the use of the Internet facilities.

Signature of Person with Parental Responsibility:
Date:

Parents' Consent for Web Publication of Work and Photographs

I agree that, if selected, my child's work may be published on the School Web Site.
I also agree that photographs that include my child may be published subject to the School Rules as guided by the DCFS

Signature of Person with Parental Responsibility:
Date:

The School may exercise its right by electronic means to monitor the use of the School's computer systems, including the monitoring of web sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the School's computer system is, or may be taking place, or the system is, or may be being used for criminal purposes, or for storing text or imagery which is unauthorised or unlawful.

Appendix 4:

GUIDANCE NOTES FOR STAFF USE OF THE INTERNET

The School computer system provides internet access to Pupils and Staff. This Responsible Use Statement will help protect Pupils, Staff and the School by clearly stating what is acceptable and what is not. These rules also apply to the use of school laptop computers at home.

- Access must only be made via the user’s authorised account and password, which must not be given to any other person.

- School computer and internet use must be appropriate to the pupil’s education, or to Staff professional activity.

- Copyright and intellectual property rights must be respected.

- Users are responsible for E-mails they may send and for contacts made.

- E-mails should be written carefully and politely. As messages may be forwarded, E-mail is best regarded as public property.

- Anonymous messages and chain letters must not be sent.

- The use of public chat rooms is not allowed.

- The school Computing system may not be used for private purposes, unless the Head teacher has given permission for that use.

- Use for personal financial gain, gambling, a political purpose, or advertising is forbidden.

- The security of the Computing system must not be compromised, whether owned by the school or by other organisations or individuals.

- Irresponsible use may result in the loss of internet access.

The School may exercise its right by electronic means to monitor the use of the School’s computer systems, including the monitoring of web sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the School’s computer system is, or may be taking place, or the system is, or may be being used for criminal purposes, or for storing text or imagery which is unauthorised or unlawful.

NAME OF MEMBER OF STAFF …………………………………………………..

Signed ……………………………………………..   Date……………………………