ONLINE SAFETY POLICY

Whole School and EYFS

Version	1	2	3		
Policy reviewed on	October 2018	September 2019	September 2021		
Policy written by	Mrs Walker	Mrs Walker	Mrs Walker		
Policy seen by Governor on (date / signature)	Mrs Wilcox	Mrs Wilcox	Mrs Wilcox		
Date of next review	September 2019	September 2021	September 2023		

This school is committed to safeguarding and promoting the welfare of children and young people/vulnerable adults and expects all staff and volunteers to share this commitment.

INTRODUCTION AND PRINCIPLES

Technology has transformed the process of teaching and learning inside schools. It is a crucial component of every academic subject and is also taught as a subject in its own right. All of the School's classrooms are equipped with interactive projectors and computers. All our pupils are taught how to research on the internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution.

Technology also plays an important part in the lives of all young people outside school. Sophisticated games consoles, like Xbox, PlayStation, Wiis and Nintendo DS, together with internet enabled mobile phones and smartphones provide unlimited access to the internet, to SMS messages, to blogging (web logging), to social media websites (like Twitter), to Skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms and other social networking sites (such as Facebook), and video sharing sites (such as YouTube). This communications revolution gives young people unrivalled opportunities. It also brings risks.

It is the duty of the School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and subtler risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school may include:

Websites; · Email and instant messaging; · Blogs; · Social networking sites; · Chat rooms; · Music / video downloads; · Gaming sites; · Text messaging and picture messaging; · Video calls; · Podcasting; · Online communities via games consoles; and · Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use of IT and Remote Working Policy (for all staff and visitors), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies

- Bullying Policy;
- Behaviour Policy
- Bring Your Own Device BYOD Policy;
- Safeguarding Policy
- Staff Code of Conduct Policy;
- Health and Safety General Policy;
- Staff Handbook
- PSHEE Scheme

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At the School we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

SCOPE OF THIS POLICY

This policy applies to all members of the School community, including staff, pupils, parents and visitors, who have access to and are users of the School's IT systems. In this policy 'staff' includes teaching and non-teaching staff, directors, advisors, and regular volunteers. "Parents" includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

This policy covers both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

ROLES AND RESPONSIBILITIES

The Governing Body/The Board

The Board Level Lead for Safeguarding with the DSL in their report for their annual review of Safeguarding the considers the safer use of electronic devices, social media and the internet and advice on who to turn to for help, are properly addressed through the curriculum and schemes of work; the review considers whether appropriate IT filters and monitoring systems are in place to prevent children from accessing harmful or inappropriate material.

Head Teacher and the School Management Team

The Head Teacher is responsible for the safety of the members of the School community and this includes responsibility for online safety. The Head Teacher has delegated day-to-day responsibility to the online safety co-ordinator who has responsibility for ensuring this policy is upheld by all members of the school community. In particular, the role of the Head Teacher and the Senior Leadership team is to ensure that: · staff, in particular the online safety coordinator are adequately trained about online safety; and safety about the use of the internet · staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the School.

Online safety coordinator

The School's online safety coordinator (Bursar/DSL) is responsible to the Head Teacher for the day to day issues relating to online safety. The online safety coordinator, has responsibility for ensuring this policy is upheld by all members of the School community, and works with IT staff to achieve this. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority's safeguarding agencies.

IT Support

The School has appointed 'Computeam' to maintain a safe technical infrastructure at the School and to keep abreast with the rapid succession of technical developments. Working in conjunction with Computeam the School is responsible for the security of the School's hardware system, its data and web filtering and for training the School's teaching and administrative staff in the use of ICT. The School's internet access is filtered by Baracuda and additional filtering and monitoring reports are provided. The use of the internet and emails, and maintenance of content filters is monitored by the online safety co-ordinator who receives reports on inappropriate usage and reports to the Head Teacher as necessary. Bursar carries out checks on student accounts for inappropriate usage, reporting to the online safety coordinator and the Head Teacher as necessary.

Teaching and support staff

As part of the induction process, all staff are required to sign a form stating that they are familiar with the School's suite of Child Protection and Safeguarding policies which includes acceptable use of social media and the School's IT systems and that they are familiar with the School's staff handbook. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

Pupils

Pupils are responsible for using the School's IT systems in accordance with the School: Pupil's participate in an Agreement for the Acceptable IT.

Parents and carers

The School believes that it is essential for parents to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

All Parents and carers are responsible for endorsing the School's ICT safety measures and the Pupil Agreement for the Acceptable Use of IT

STAFF AWARENESS AND TRAINING

Education and training

1. **Staff: awareness and training**

New staff receive information on school's online safety and Acceptable Use of IT and Remote Working practices as part of their induction.

All staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All specialist staff also receive our online safety Policy on arrival at school. Agency staff providing short-term cover (which may only be provided for a day or part of a day will be requested to peruse a summary sheet of information and to refer to the DSL for all guidance). Where such cover extends beyond three weeks the agency staff member will be expected to fulfil all the requirements expected of staff in permanent employment

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. These behaviours are summarised in the School: Pupil Agreement for the Acceptable Use of, I.T. which must be signed by pupils and a parent and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

A record of concern should be entered on the Online safety Incident log by a staff member as soon as possible if any incident relating to online safety occurs and be provided directly to the online safety coordinator who will then liaise with the Head Teacher in their capacity as DSL. Concerns will be dealt with in accordance with the School's Safeguarding Policy.

2. Pupils:

Online safety in the curriculum IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHEE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHEE pupils are taught about their online safety responsibilities and to look after their own online safety and of their duty to report any such instances they or their peers come across. Pupils can report concerns to any member of staff at the School.

Pupils should be aware of the impact of cyber-bullying and the risks posed by adults or young people, who use the internet and social media to bully, harass, groom, abuse or radicalise other people Pupils should know how to seek help if they are affected by these issues (see also the School's Bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying (including cyberbullying)). Pupils should approach the DSL as well as parents/guardians, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents

The School seeks to work closely with parents and guardians in promoting a culture of online safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The School therefore arranges occasional events which parents are invited to attend when an outside specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Policy Statements

1. **Use of school and personal devices**

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

• Staff are referred to the Bring Your Own Device (BYOD) Policy for further guidance on the use of non-school owned electronic devices for work purposes.

The School's policy on the use of mobile phones and cameras is set out in detail in the School's Mobile Phones and Cameras Policy. Staff are only permitted to use their personal mobile devices on a restricted basis:

• Staff must have their personal devices switched to silent during the working day.

• They may only use such devices during break-times and lunchtimes either in the school staffroom or in their classroom only when no children are present.

• Staff who wish to take photographs or video of pupils must use a school device. Staff must never use their personal mobile device for filming/taking photos of children.

• Staff who act in breach of this policy may be subject to disciplinary action.

• Personal telephone numbers, email addresses, social media or other messaging systems may not be shared with pupils or parents / carers under any circumstance.

• Under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Pupils

We do not allow pupils to bring mobile phones into school unless it is authorised on an individual basis.

If pupils bring in mobile devices (e.g. for use during the journey to and from school) they must be handed in to the Bursar’s office or their class teacher at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. Access to school mobile technologies available for pupil use is via the class teacher

The School recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the SENDCo to agree how the School can appropriately support such use. The SENDCo will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or in the classroom at break times when no children are present.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the School. Staff personal social media accounts should not have a public profile setting.

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that email communications through the School network and staff email addresses can be monitored.

Staff must immediately report to the online safety coordinator / Computeam (the IT Manager) the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails (phishing emails) and should report emails they suspect to be fraudulent to Computeam.

Any online communications must not either knowingly or recklessly:

· place a child or young person at risk of harm, or cause actual harm;

· bring the School into disrepute;

· breach confidentiality;

· breach copyright;

· breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

§ making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;

§ using social media to bully another individual; or

§ posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media. Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The School ensures that staff have access to their work email address when offsite, for use as necessary on school business. Staff are reminded that parents are not permitted to use their mobile phones or camera in or around the EYFS setting without prior approval from the Head Teacher.

Pupils

Remote Learning

Pupils in KG1-F4 use Class DoJo and F5-F6 use Microsoft Teams. All guidance in this policy refers to the use of these platforms

Pupils in F5 and F6 are issued with their own personal Teams Account for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Pupils should be aware that communications through the School network and school email addresses are monitored.

All other pupils have access to the internet which is controlled.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the online safety coordinator for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the online safety coordinator or the DSL or another member of staff.

The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of (a violent or sexual) nature directly to a member of staff who will report the incident to Soft Egg and also inform the online safety coordinator. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the School's Behaviour Policy. Pupils should be aware that all internet usage via the School's systems and its Wi-Fi network is monitored.

3. Data storage and processing

The School takes its compliance with the General Data Protection Regulations and the Data Protection Act 2018 seriously. Please refer to the Privacy Notice for further details. Staff data handling procedures are set out in the Staff Data Protection and Handling policy found in the Staff Handbook. Staff and pupils are expected to save all data relating to their work to school central servers / Google Drive Account/Engage management information system. Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal devices or personal memory sticks; only school owned encrypted memory sticks may be used. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head teacher and the online safety coordinator who will liaise with Computeam as appropriate.

4. Password security

Staff have individual school network logins and email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security. The School's IT system forces all users to change their password every 120 days, with the exception of pupils' network passwords which are allocated to them by the School IT provider Computeam.

All pupils and members of staff should:

· use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers).;

· not write passwords down; and

· not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at **school events only** for their own personal use. To respect everyone's privacy and in some cases for child protection reasons, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others, unless under the supervision of the class teacher. Written permission from parents or carers will be obtained before photographs of pupils are used in any external publication. Photographs that include pupils which are published on the School website, or displayed elsewhere, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

The School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the Local Authority's safeguarding agencies. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the School's policies and procedures (in particular the Safeguarding Policy).

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Bullying Policy.

Complaints

As with all issues of safety at the School if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the class teacher in the first instance, who will liaise with the Head Teacher who will undertake an investigation. Please see the Complaints Policy for further information.

APPENDX 1

Guidance for keeping pupils safe online.

1. **General principles**

Pupils may conduct research, learn, and communicate with others. All pupils agree to follow the rules of appropriate behaviour: ● Pupils may not copy material and claim that they wrote it. ● Pupils will visit only internet sites suitable for children and for educational purposes.

2. **Privileges**

The use of school computers is a privilege. The teachers decide when students may use computers or the internet. If a pupil uses a computer or the internet in ways that are not appropriate, they may have privileges taken away. Also, remember that computer files are not private. School and system administrators can view your work.

3. **Etiquette**

Pupils will follow rules for appropriate behaviour. Some (but not all) of those rules are listed below: ● Be polite when writing. ● Use appropriate language. ● Pupils may use computers for research, but must identify where information is found. ● Do not share account or password information with others, and do not try to log on as someone else. ● Do not try to see the folders, work, or files of others. ● Do not use or share anything which is offensive, upsetting or sexual in nature or likely to offend or upset another person, both verbal and pictorial.

4. **Online Safety**

Please follow these rules to stay safe online ● Do not give your phone number, home address or email address to anyone over the internet. ● Do not become “friends” or chat to anyone online if you have not met them in real life. ● Do not send images of yourself to anyone if you have not met them in real life. ● Never agree to meet someone you have only “met” online. ● Notify an adult immediately if you find information on the computer that makes you uncomfortable or nervous.

5. **Truthfulness**

The School is not responsible for the truth or the quality of the information found on the internet.

6. **Privacy**

Your information and records of what you viewed, received and saved are not private. Teachers and technical staff may review files to be sure everyone is using computers responsibly.

7. **Security**

Security on any computer system is important. If a student knows of any times when these rules are broken, they must tell a teacher. School personnel are in charge of internet access. Pupils must not connect to the internet unless directed to do so under the supervision of a teacher. Do not tell anyone else your password and do not log in as anyone else.

8. **Filtering**

The School uses software to filter or block material harmful to children. Pupils should not attempt to get around filters.

9. **Vandalism**

Any vandalism will result in the loss of privilege to use the internet, and/or the computers, themselves. Vandalism includes: ● physical damage to the computers ● damage to files that belong to others ● changing any computer settings or software ● any attempts to bypass security settings

10. **Mobile technology including mobile phones outside of school hours**

• The use of mobile phones in the School is not allowed. If you bring a phone to school because you are travelling to and from school alone then this must be handed in to your teacher or the School office at the beginning of the day. • Please remember that the etiquette and online safety guidelines in this agreement apply to the use of mobile phones and also outside of school hours. • If the School discovers that a pupil's online behaviour or use of mobile phone apps, outside of school, has broken this agreement then the School will apply its Behaviour and Anti bullying policies to deal with this.

11. **Consequences**

Violations of any of these rules may result in the loss of access to the School systems and your parents will be informed. There may also be disciplinary actions that your teacher will determine are appropriate consequences to violating the Acceptable Use rules.