Messingham Primary School
Online Safety Policy

At Messingham Primary School we believe that all children should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to both staff and children, for example:

- Access to world-wide educational resources.
- Access to experts in many fields.
- Access to learning wherever and whenever convenient.

Managing the Internet Safely

There is a requirement in all schools to provide as safe an Internet environment as possible and to teach children to be aware of and respond responsibly to any risk.

Technology and Infrastructure

Internet filtering is a key service and the school has adequate approved filtering, anti-virus, anti-spam ware and firewall solutions installed on the network.
Messingham Primary School will therefore;

- Maintain connection to a filtered broadband. We purchase this through the local authority.
- Have additional user-level filtering in place.
- Ensures network health through the use of appropriate anti-virus software and regular technical checks.
- Ensure technical staff and administrators are up-to-date with services and policies.
- Never allow children to access internet logs.
- Use individual network logins for staff

Policy and Procedures

Due to the international scale and nature of the information available via the Internet, it is not always possible to guarantee that unsuitable material will never appear. Awareness of the risks, having the appropriate systems in place and supervising children in their use of the Internet are important considerations in reducing such risk. Therefore Messingham Primary School will;

- Supervise children's use of the internet at all times, and exercise extra vigilance on occasions when they have more flexible access, either by physical staff presence or use of a filtering and electronic monitoring system.
- Use an appropriate and approved filtering system which blocks harmful and inappropriate sites.
- Exercise extra vigilance during raw image searches.
- Inform children that Internet use is monitored.
- Inform all users that they must report any failure of the filtering systems to the system administrator.
- Require children and staff to sign an acceptable use agreement form which is fully explained to them.
- Make the 'rules of appropriate use' clear to all users, at an appropriate level, and what sanctions will result from misuse.
- Keep a record of any cyber bullying or inappropriate behaviour when using IT equipment for evidence in line with the school Behaviour Policy.
- Ensure the designated DSL has appropriate training in e-safety.
- Ensure parents/carers provide consent for their child to use the Internet, as well as other ICT technologies. This will form part of the acceptable use agreement.
- Make information on reporting offensive materials, abuse, bullying etc. available to children, parents, carers and staff.
- Immediately refer any material we suspect is illegal to the appropriate authorities.
- Ensure staff are aware of signs of children being influenced by others on the internet e.g. through Prevent training.
- Pupils' full names will not be used on the school's social media.
- Staff must sign out any equipment they take to a different place. This is kept on the back of the door in the IT cupboard. There should also be a signing out book in every classroom. If staff want to take equipment out of school permission must be given by the head teacher.
- Teaching staff are allocated a laptop which must not be passed on to another member of staff without agreement with either the admin assistant, the computing lead or the head teacher.

- School devices can be taken on school trips but will not connect to the internet. If devices are going to be sent home with pupils, parents will sign an agreement before hand.
- Permission from parents/carers will be obtained before images of pupils are electronically published.
- Mobile phones are not allowed in school for pupil use without the teacher's permission. If they are brought to school by pupils, they must be handed in to an adult and locked away until home time.
- Every device has a security number and is on the school inventory. This is to ensure that devices don't go missing. Spot checks are carried out each term to ensure devices are in the appropriate place. The inventory is update when needed.
- Staff should not use each others' emails and if using shared computers must log out and delete any downloads.
- Sensitive data will not be stored on devices unless they are encrypted.
- Staff must ensure that communication devices e.g. chrome books, laptops, iPads etc. are locked away every evening.

How will online safety complaints be handled?

- Complaints of internet use, including but not exclusively cyber bullying and sexting, will be dealt with by a senior member of staff. Parents will be informed if it is deemed to be appropriate to do so.
- If school equipment is used for these purposes, will either be disconnected from the internet or it will be taken off them for 1 week depending on the nature of the incident. If this is a misuse of the internet, the internet will be blocked. If it is a misuse of a device, the device will be removed.
- Incidents outside of school should be reported to the head teacher who will follow the behaviour and anti-bullying policy following investigation.
- Any complaint about staff misuse must be referred to the head teacher who will follow the appropriate procedures.
- Further advice will be sought in the event of potentially illegal use of the internet.

Education and Training

Even with all safety procedures in place, children will still occasionally download inappropriate material. Children and staff need to know how to respond responsibly. Messingham Primary will therefore;

- Foster a 'No Blame' environment that encourages children to tell an adult immediately they encounter any material they feel uncomfortable with.
- Ensure children and staff know what to do if there is a cyber bullying incident, including peer on peer abuse.
- Ensure all children know how to report abuse.
- Have an e-safety education programme throughout all Key Stages, which is part of the Computing curriculum (including an e-safety day in February). Through this children are taught a range of skills and behaviours relevant to their age and experience.
- The age-appropriate acceptable use policy agreement will be posted in each classroom.
- Ensure, when copying materials form the web, children and staff, understand issues of plagiarism and copyright.
- Offer e-safety advice and guidance for parents / carers.
- Pupils will be informed that network and internet use will be monitored by class teacher and computing leader. A log of checks made will be kept by CR.

Remote Learning

- Children have been given their own username and password in order to access their Google Classroom account in order to access their learning online.
- Staff have had sufficient training on Google Classrooms.
- Parents and children are aware of the online safety expectations which are listed on the Google Classrooms Internet Safety Agreement.
- Any incidents to be reported to the head teacher and computing lead.

Next Review Date: September 2021