

Manford Primary School

Online Safety Policy



‘Believe in yourself’

Approved by:

L James

Date: July 2025

(To be verified by
Governors)

Last reviewed on:

July 2025

Next review due by:

September 2026

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents about online safety	7
6. Cyber-bullying.....	7
7. Acceptable use of the internet in school.....	10
8. Pupils using mobile devices in school.	10
9. Staff using work devices outside school.....	11
10. How the school will respond to issues of misuse.....	11
11. Training.....	11
12. Monitoring arrangements	12
13. Links with other policies	12
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers).....	13
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers).....	14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	15
Appendix 4: KS1 online safety agreements.....	16
Appendix 5: KS2 online safety agreement	17
Appendix 6: Online safety information for parents, to be given in the welcome pack.....	19
Appendix 7: online safety training needs – self-audit for staff.....	20
Appendix 6- Example of the Online safety scheme of work we follow- 2BeSafe- Being Safe in a Digital World	22

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalization, extremism, misinformation, disinformation and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users, such as child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Chair of Governors oversees online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring

- Ensuring that any online safety incidents are logged on CPOMS (Online Safeguarding) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 7 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board. Monthly reports will be created from CPOMS and discussed in SLT, further action will be decided

This list is not intended to be exhaustive.

3.4 The ICT Manager/ComputerTalk

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material (LGFL, SOPHOS, SENSO and Meraki)
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a **monthly** basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendix 1, 2, 4 & 5)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing immediately.
- Following the correct procedures by speaking with the IT lead if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1). This is given to parents in the welcome pack and the aim is for every child to have read this with their parents and signed it.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum ([National Curriculum computing programmes of study](#), [guidance on relationships education, relationships and sex education \(RSE\) and health education](#))

All schools have to teach:

- [Relationships education and health education](#) in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Specific online safety lessons will take place throughout every half term; these are taken from Purple Mash- 2BeSafe in a Digital World scheme of work which follows the eight strands of the document '[Education for a connected world](#)'. Lessons will be mapped across the year.
- Switched on Computing scheme of work is now used by Years 5 and 6, Purple Mash Scheme being followed from Reception to Year 4, and online safety is fully mapped.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Specific online safety lessons will take place throughout every half term; these are taken from Purple Mash- 2BeSafe in a Digital World scheme of work which follows the eight strands of the document '[Education for a connected world](#)'. Lessons will be mapped across the year.
- Switched on Computing scheme of work is now used by Years 5 and 6, Purple Mash Scheme being followed from Reception to Year 4, and online safety is fully mapped.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. Also through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' workshops and parents evenings when appropriate.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.2a Guidance for staff:

*“Bullying can be done verbally, in writing or images, **including through communication technology (cyber bullying) e.g. graffiti, text messaging, e-mail or postings on websites.** It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.”*

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Report the incident to the DSL
2. Advise the child not to respond to the message
3. Refer to relevant policies including online safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
4. Secure and preserve any evidence
5. Inform the sender's e-mail service provider
6. Notify parents of the children involved
7. Consider delivering a parent workshop for the school community
8. Consider informing the police depending on the severity or repetitious nature of offence
9. Inform the online safety officer

Radicalisation.

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. The Counter-Terrorism and Security Act 2015 places a duty on schools (and other specified authorities) to have due regard to the need to prevent people from being drawn into terrorism. Radicalisation is usually a process not an event – it is possible to intervene to prevent vulnerable people being drawn into terrorism. Vulnerable individuals identified as being at risk of radicalisation are referred to the Channel programme. This is a multi-agency panel that provides support through specialised intervention providers. Whilst the risk of radicalisation is remote it is still a possibility to consider when assessing behavioural changes.

All concerns should be reported to the DSL.

Advice regarding Prevent or referrals to the Channel programme can be obtained from:

The Prevent Co-ordinator for Redbridge who is based in LBR Community Safety and can be contacted via prevent@redbridge.gov.uk or 020 8708 5971.

If there is risk of immediate harm or danger then you should contact the police on 999 or the Police Anti-Terrorist Hotline 0800 789 321

(Linked to the child-protection and safeguarding policy)

'As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress'

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. Report to and discuss with the named DSL or deputies
2. Advise the child on how to terminate the communication and save all evidence
3. Contact CEOP <http://www.ceop.gov.uk/> (Child Exploitation & Online Protection Centre - internet safety - CEOP)
4. Consider the involvement of the police and social services

'Children should be confident in a no- blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.'

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Any searching of pupils will be carried out in line with:
 - The DfE's latest guidance on [searching, screening and confiscation](#)
 - UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Manford Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Manford Primary School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2 & 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

At the start of every school year class teachers revisit the rules for keeping safe on the internet. Pupil's agree and sign class online safety agreements, see appendix 4 & 5.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1, 2 & 3.

8. Pupils using mobile devices in school.

Pupils within KS2 may bring mobile devices into school if they are needed due to travelling to school independently, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 2).

Any mobile phone belonging to a pupil is switched off and stored in the class lock box until the end of the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of [three random words](#), in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device is locked if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3 and the separate Acceptable Use Policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. All incidents will be recorded on CPOMS under the category online safeguarding.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL/ reporting staff member logs behaviour and safeguarding issues related to online safety on CPOMS. An incident report log will be printed and discussed monthly with SLT, but is accessible at all times.

This policy will be reviewed every year by the Online Safety Co-ordinator. At every review, the policy will be shared with the governing board.

The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy
- Schools disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Anti-bullying policy
- Image and photo policy
- Whistle blowing policy
- Acceptable Use policy
- Email Policy

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	Date:
------------------------	--------------

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	Date:
-------------------------------	--------------

(To be given to new parents and in the welcome pack)

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

 (To be given to new parents and in the welcome pack)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	Date:
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

The 14 page policy must be read and the form below signed in agreement.

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

The school may exercise its right to monitor the use of the school’s information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the staff ‘Acceptable Use’ policy.

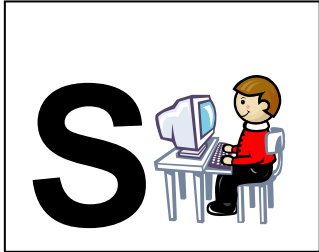
I will adhere with this policy and I understand that if I become aware of a data breach or the potential for a data breach caused either by myself or by another individual I MUST inform the Headteacher or Designated Data Protection Lead immediately.

Full name (printed):

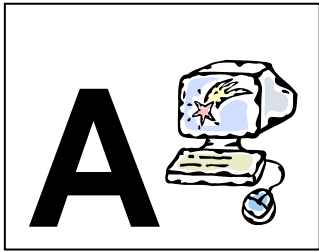
Signed:

Date:

Think before you click



I will only use the Internet and email with an adult



I will only click on icons and links when I know they are safe



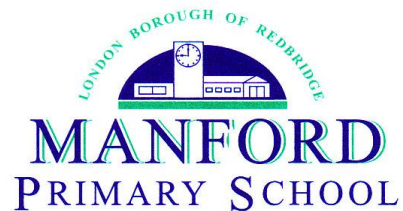
I will only send friendly and polite messages



If I see something I don't like on a screen, I will always tell an adult

Class: _____ Date: _____

Appendix 5: KS2 online safety agreement



Online Safety agreement form: KS2
Keeping safe: stop, think, before you click



Class: _____

Year: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, iPads, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way.

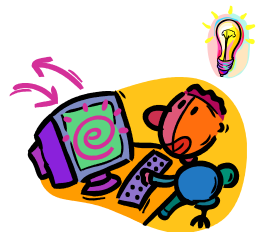
I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer.

Pupils signatures: _____

_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Date: ___/___/___

Keeping safe: stop, think, before you click!
12 rules for responsible ICT use



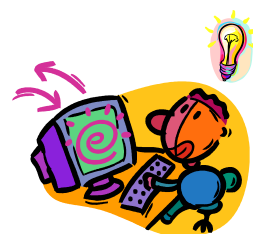
These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers/iPads for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.

- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Appendix 6: Online safety information for parents, to be given in the welcome pack

Online Safety – helping your child stay safe



The best way to help your child to be a safe when using the internet and new technologies is to talk to them and make sure they understand these simple rules:

- You should never give out personal details to online ‘friends’. Use a nickname when logging on and don’t share full name, email address, mobile number, school name and any photos, including photos of family or friends – any picture or video online can be changed or shared without permission.
- Talk to your child about what they are doing online and who they are talking to. Get them to show you how to use things you are not familiar with. Keeping the computer in a family room means that you can share your child’s online experience, they are less likely to act inappropriately (i.e. via webcam) and their online ‘friends’ will see they are in a family room.
- If your child receives a message that upsets them, remind them not to reply, they should save the message and show you or another trusted adult.
- Spam and junk emails and texts are not true, don’t reply or send them to anyone else, just delete them.
- Don’t open files sent from people you don’t know. They could contain a virus, or worse – an inappropriate image or film.
- An online ‘friend’ is anyone you have not met in real life; no matter how long you have been friends with them.
- Help your child to understand that some people lie online and that it’s better to keep online ‘mates’ online. They should never meet up with any online ‘friends’ without an adult they trust.
- Make sure they know how to block someone online and report them if they feel uncomfortable.

Make sure your child feels able to talk to you, let them know that it’s never too late to tell someone if something makes them feel uncomfortable. Don’t blame your child, let them know you trust them.

Useful websites:

<https://parentsafe.lgfl.net/>

www.ceop.gov.uk

www.thinkuknow.co.uk

www.getnetwise.org

www.childnet.com/parents-and-carers

Appendix 7: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)

ONLINE SAFETY TRAINING NEEDS AUDIT

Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6- Example of the Online safety scheme of work we follow- 2BeSafe- Being Safe in a Digital World



	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and Lifestyle	Privacy and Security	Managing Online Information	Copyright and Ownership
Lesson 1	I can recognise, online or offline, that anyone can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who makes them feel sad, uncomfortable, embarrassed or upset.	I can recognise some ways in which the internet can be used to communicate.	I can identify ways that I can put information on the internet.	I can describe ways that some people can be unkind online.	I can identify rules that help keep us safe and healthy in and beyond the home when using technology. I can give some simple examples of these rules.	I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location).	I can talk about how to use the internet as a way of finding information online.	I know that work I create belongs to me.
Lesson 2		I can give examples of how I (might) use technology to communicate with people I know.		I can offer examples of how this can make others feel.		I can describe who would be trustworthy to share this information with. I can explain why they are trusted.	I can identify devices I could use to access information on the internet.	I can name my work so that others know it belongs to me.
Total	1	2	1	2	1	2	2	2