Westfield Primary Community School

Online Safety Policy

Approved By:	School Improvement Committee
Date:	October 2022
Review Date:	October 2025

Vision for Westfield

Together we strive to:
Inspire *a love for our community through mutual respect, teamwork and the shared belief that anything is possible*

Create *a learning culture which recognises potential, celebrates achievement and respects individuality*

Nurture *strong relationships in a safe and secure environment, where opinions are valued and kindness is the core*

Contents

---

1. Aims

Our school aims to:

- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Set out expectations for all Westfield community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures 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, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Scope

This policy applies to all members of the Westfield Primary community (including staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

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 and our current scheme of work iCompute.

3. Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school.

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 monitor online safety incidents through updates provided in the termly Headteacher's report to governors. The School Improvement Committee will monitor the curriculum design and implementation.

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 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 Safeguarding and Child Protection policy.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the curriculum leaders, SLT, Vital 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's Safeguarding and Child Protection policy
- Ensuring that any incidents of online bullying are recorded on CPOMs and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety to the governing board through the termly Headteacher's report

3.4 The School's ICT provider (Vital)

Vital manage our windows system which is hosted in a secure data centre. They also manage our Google workspace system and provide us with full IT support.

Vital is responsible for managing our server, chromebooks and ipads through:

- Providing reliable hardware, which is appropriate for education, (eg desktop PCs, laptops, chromebooks or iPads) and associated peripherals
- The initial set-up, delivery, installation and disposal of all waste
- Ongoing support and personal service from an assigned technician
- Proactive and reactive technical support
- Accidental damage cover
- Providing advice and input on project work including refurbishments and moves

- Refreshing hardware every three years
- Putting in place an appropriate level of security protection, 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
- 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.5 Broadband Provider – North

North is responsible for managing our broadband service through:

Security, safeguarding and Filtering

- Internet filtering by group, user or device
- Https inspection
- Layer 7-application control
- Firewall and intrusion prevention
- Configurable monitoring and reporting functions
- Anti-virus and malware protection for web content
- Transparent proxy
- Remote access
- Site to site VPN

Service and maintenance

- Service desk, including site visits by DBS checked engineer when required
- Maintained equipment
- Service Level Agreement
- A pro-active monitoring service

3.6 All staff and volunteers

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

- Understanding that online safety is a core part of safeguarding; as such it is part of everyone's job.
- Reading, consistently following and maintaining an understanding of this policy in conjunction with the school's Safeguarding and Child Protection policy.
- Identifying opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.
- Whenever overseeing the use of technology (devices, the internet, remote learning, all other technology in school or setting as homework tasks, encouraging sensible use, monitoring what pupils are doing and considering potential dangers and the age appropriateness of websites.
- Carefully supervising and guiding pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant).

- Notifying the DSL (or deputies) of new trends and online issues so awareness can be shared across school.
- Modelling safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and offsite, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- 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 (Appendices 1 and 2).
- Responding to and recorded all online-safety incidents in the same way any other concern or safeguarding incident would be.
- 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'.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

3.7 Parents

Parents are expected to:

- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or unkind comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Notify a member of staff of any concerns about their child's use or experiences of online activity or technology.
- Support the terms outlined the pupils' Acceptable Use Agreements (Appendices 1 and 2)

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

3.8 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).

All visitors and members of the community have a responsibility to report any concerns, no matter how small, to the designated safeguarding lead and to model safe, responsible and professional behaviours in their own use of technology

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The objectives below are taken from the National Curriculum computing programmes of study.

It is also taken from the 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

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

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 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.

iCompute

At Westfield Primary Community School, we use the iCompute scheme of work. iCompute is fully mapped to the National Curriculum for Key Stage 1 and Key Stage 2 and is designed for mastery. The curriculum provides rich and varied learning experiences for pupils throughout the primary phase with progressive, sequences of lessons from EYFS to Year 6. Step-by-step lesson plans support teachers and subject leaders develop expertise and skills, which ensures that the curriculum has impact; with pupils being engaged, challenged and making excellent progress in all aspects of their computing education.

Natterhub

To support our children's understanding of online safety, we use Natterhub. This is a safe, gated educational social media platform for primary schools, with weekly interactive lessons on all aspects of online safety for Years 1-6. It looks and functions like 'real' social media but it is gated to the school environment, meaning that children can explore and play in a safe, online space to properly understand the benefits and potential pitfalls of social media.

Natterhub lessons are mapped against the new compulsory Relationships and Health Education (RSHE) curriculum, as well as the UKCIS 'Education for a Connected World' document and government guidelines including the Online Harms White Paper.

Please see Appendix 4 for curriculum coverage.

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.

If parents 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 a person or group by another person or group, where the relationship involves an imbalance of power.

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.

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

In relation to a specific incident of cyber-bullying, the school will follow use the school's 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.

6.3 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, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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 cooperation

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 head teacher 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 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.

7. Acceptable use of the internet in school

All pupils, 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 -3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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 to ensure they comply with the above.

More information is set out in the Acceptable Use Agreements (Appendices 1 - 3)

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day.

There may be exceptional circumstances where children may need to use their mobile phone for medical reasons but this is agreed on an individual basis.

Any use of mobile devices in school by pupils must be in line with the Acceptable Use Agreement (see Appendices 1 and 2).

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.

Pupils are expected to switch off their mobile phone before entering the school gates, hand them in to a member of staff on entering the building and not switch them back on until exiting the site.

All mobile phones are stored securely throughout the school day. The school takes no responsibility for any loss or damage to phones or other electronic devices brought into school.

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 devices password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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 locks if left inactive or unattended 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 devices in any way which would violate the school's terms of acceptable use, as set out in Appendix 3.

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 Vital – our ICT provider.

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 our behaviour policy and log incidents on CPOMS. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 code of conduct. 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, staff briefings 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 other children 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 Safeguarding and Child Protection policy.

12. Monitoring arrangements

All staff are responsible for raising and recording behaviour and safeguarding issues related to online safety. A separate category on CPOMS allows incidents relating to online safety to be continuously monitored and evaluated.

This policy will be reviewed every two years. At every review, the policy will be shared with the governing board. The review will consider and reflect upon 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
- Staff Code of Conduct
- Behaviour policy
- Pupil Remote Learning Policy
- Information Policy
- Complaints Policy
- Acceptable Use Policy
- Disciplinary Policy
- Privacy Notices
- Information Security Incident Reporting Policy

Appendix 1: EYFS and KS1 Acceptable Use Agreement

Westfield Primary Community School

Acceptable Use Agreement

I will always ask permission before using the Internet and will think about the website I use.

I will ask for help if something pops up that I do not understand.

Any messages I send will be polite and sensible.

I will never give out personal details like my name, home address or telephone number.

I will always tell an adult if I see anything I am unhappy with or receive messages I do not like.

I know the school will check my emails, files and Internet sites I visit.

I know if I deliberately break the rules it may result in me not being allowed to use the Internet, computers or devices.

I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers but NOT other pupils.

If I find a website or image that upsets me, I will tell a teacher straight away.

I will not logon using another person's account (with or without their permission.)

I will take care when using the computers and other school equipment.

Signed Pupil: _____ Date: _____

Signed Teacher: _____ Date: _____

Appendix 2: KS2 Acceptable Use Agreement

Westfield Primary Community School

Acceptable Use Agreement

I will always ask permission before using the Internet and will think about the website I use.

I will not ignore pop up boxes I do not understand.

Any messages I send will be polite and sensible.

I will never give out personal details like my name, home address or telephone number.

I will always tell an adult if I see anything I am unhappy with or receive messages I do not like.

I will not search for offensive material.

I know the school will check my emails, files and Internet sites I visit.

I know if I deliberately break the rules it may result in me not being allowed to use the Internet, computers or devices.

I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers but NOT other pupils.

If I find a website or image that is inappropriate, I turn off the monitor and I will tell my teacher straight away.

I will not logon using another person's account (with or without their permission.)

Internet access is a privilege, not a right and that access requires responsibility.

I will take care when using the computers and other school equipment.

I will not install any software or hardware (including memory sticks) without permission from a teacher.

Signed Pupil: _____ Date: _____

Signed Teacher: _____ Date: _____

Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable Use Procedure for All Staff - including temporary or supply staff and visitors to school.

As a member of staff, either temporary or permanent, or a visitor to the school I recognise that it is my responsibility to follow school procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils or download any pupil information
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned.
- I will delete photographs from devices as soon as they have been added to tapestry/used in class
- I will not give my personal contact details such as email address, mobile phone number, social media account details to any pupil in the school. Contact will always be through a school approved route. I will not arrange to video conference or use a web camera with pupils unless specific permission is given.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorized system manager.
- I will not befriend school age pupils, past or current on social media.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date.
- I will only use my mobile phone in class to access emails. It will be kept on silent mode during lessons except in an emergency situation and permission given from a senior leader.
- I will not use the school network for accessing my personal social media.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded and will report any incidents of concern regarding children's safety (including unsuitable materials or inappropriate activity) to the Headteacher.
- If I have access to any confidential school information, pupil information or data it will only be removed from the school site with permission and if so, it will be carried on a device given to me by the school. I will report immediately any accidental loss of confidential information to a senior member of staff so that appropriate action can be taken
- I will respect copyright and intellectual property rights.
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff.
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.
- I understand that the school may monitor or check my use of ICT equipment and electronic communications to ensure policy compliance.

Signed……. Date…….

Appendix 4: Curriculum Coverage

Online Safety – Y1 and Y2
Online Safety should be part of daily discussions in the classroom and addressed whenever technology is used. iSafe: - understand what being online may look like, the different feelings we can experience online - how to identify and approach adults who can help - understand that people online may try to manipulate others, how this can make someone feel and how to approach adults who can help. - understand photos can be shared online - understand the importance of seeking permission before sharing photos of others online - understand what personal information means - understand that personal information is unique to themselves - understand personal information should be only be given to trusted adults - understand that not everyone you meet is trustworthy - begin to identity the characteristics of people who are trustworthy - understand that emotions can be a tool to help judge unsafe situations - understand the importance to checking with an adult before going online

Online Safety Y3 and Y4
Online Safety should be part of daily discussions in the classroom and addressed whenever technology is used. iSafe - empathise with those who have received mean and hurtful messages - Judge what it means to cross the time from harmless to harmful communication online - Generate solutions for dealing with cyber bullying - Identity the characteristics of strong passwords - Apply characteristics of strong passwords to create new passwords - Compare and contrast online-only friends and in person, face to face friends

- Analysis why private information should not be given to anyone online without permission from a trusted adult - Debate how to respond if an online only friend asks them personal questions

Online Safety Y5 and Y6	
Online Safety should be part of daily discussions in the classroom and addressed whenever technology is used. - Recognise the importance of never sharing passwords, except with a parents or guardians - Understand the importance of screen locks - Know how to create passwords that are hard to guess, yet easy to remember - Choose the right security for their login settings - Put what they have learnt into practice by playing online games - Identify situations of harassment or bullying online	- Learn specific ways to respond to bullying when you see it - Know how to behave if you experience harassment - Make good decisions when choosing how and what to communicate and whether to communicate at all - Identify situations when it's better to wait to communicate face to face with a peer rather than straight away - Recognising that seeking hep for yourself and others in a strength - Be aware of online tools for reporting abuse - Evaluate what is meant to be a bystander or upstander online