



Peter Gladwin

Online Safety and Social

Media Policy

Approved by: Full
Governing Body

Date: 12/3/26

Next review due by:

February 2027

Contents

1. Aims	1
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating and supporting parents/carers about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school	7
8. Pupils use of mobile devices (including smartphones) in school	8
13. Training for staff, governors and volunteers	12
11. Monitoring arrangements	13
12. Links with other policies	13

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, including mobile and smart technology (which we refer to as 'mobile phones')
- › 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

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](#)
- › [Meeting digital and technology standards](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- › [Relationships and sex education \(RSE\) and health 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, regular updates and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that 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 what needs to be done to support the school in meeting the 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 the school's safeguarding needs

All governors will:

- › Make sure they have read. and understand this policy
- › Agree and adhere to the policy
- › Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- › Make sure 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 making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) 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 making sure 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 and make sure 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 staff to make sure the appropriate systems and processes are in place
- › Working with the headteacher, ICT 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 child protection policy
- › Responding to safeguarding concerns identified by filtering and monitoring
- › Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- › Updating and delivering staff training on online
- › 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
- › Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 The ICT technician

The ICT technician is responsible for:

- › Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- › Making sure 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 All staff

All staff 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
- › Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware that they must report any incidents of those systems or processes failing by contacting the DSL
- › Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure 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'

3.6 Parents/carers

Parents/carers are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

- › What are the issues? – [UK Safer Internet Centre](#)
- › Help and advice for parents/carers – [Childnet](#)
- › Parents and carers resource sheet – [Childnet](#)

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 and expected to read and follow it.

4. Educating pupils about online safety

4.1 Pupils will be taught about online safety as part of the curriculum

All primary schools have to teach: [Relationships education and health education](#)

In **Key Stage (KS) 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 (KS) 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
- › Be discerning in evaluating digital content

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

- › That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- › How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- › That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- › The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- › Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- › That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with 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.

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

5. Educating and supporting parents/carers about online safety

The school will raise parents/carers' 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.

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 1 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, in an age appropriate way, 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 encourage them 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.

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 governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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.

6.3 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 evidence in relation to an offence

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](#)

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 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

7.1 All staff must follow the acceptable use of ICT policy

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.

All staff must adhere to the acceptable use of ICT policy.

7.2 Use of technology and screens in school

We are aware of the advice around screen time for young people (e.g. national Institute of health and care excellence) and seek to ensure that technology and screens is only used for educational purposes. Technology (computers, ipads, laptops and interactive large screens) will sometimes be used during lessons and in assemblies. These will support and enhance learning activities and may include displaying visual aids, watching short educational film clips, practising fluency skills (e.g. times tables, phonics activities), teaching ICT/coding skills. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource.

Where resources are made available to parents through online platforms (e.g. to support reading or learning times tables), then, where possible, efforts will be made to find alternatives to these (e.g. games or hard copies of books) so that parents are able to reduce or avoid pupils screen use. The impact on staff workload will be considered when making decisions regarding the feasibility of providing alternative approaches to online activities for home learning. Screens will not be used to 'occupy' children during 'wet play'. Occasionally pupils will be given opportunities to watch (parts) of films and parents will always be informed of this and given the opportunity for their child to take part in an alternative activity.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7.3 Generative artificial intelligence (AI)

Generative AI is a type of AI that can produce content such as: text, images, music, audio and videos. Although AI has the potential to reduce workload, it can generate information that appears factual but is inaccurate and must be used safely. Many AI tools collect information from users and use this to adapt the information shared. School staff may make use of AI tools (e.g. ChatGBT/Canva etc) to generate resources for use within teaching and learning, however, school staff must review and evaluate the accuracy and quality of the materials produced and must never share personal data (pupil, parents/carers or staff personal data, including digital images of children) within these websites.

The DfE guidance is that schools should not be letting primary pupils use AI as the minimum age limit for many tools is 13. Children at our school do not use AI tools during the school day. We do not expect children to use AI for homework tasks nor any other school-related work. Our online safety curriculum includes opportunities for pupils to reflect on the validity and credibility of sources of information obtained online and through AI and the potential advantages/disadvantages of using AI both for themselves and for society more widely.

8. Pupils use of mobile devices (including smartphones) in school

Pupils who walk to or from school independently sometimes choose to bring a mobile phone to a school. Pupils are required to switch these off when on school property and give these to the teacher at the start of the day where they are stored securely. Pupils' mobile phones must remain

switched off at all times whilst on school premises, except in extenuating circumstances where express permission is given by a member of the SLT. This approach ensures that all pupils are safe on school premises and enables pupils to have a mobile phone with them when they are walking home if a parent wishes.

Children's access to mobile phones has become an increasingly contentious issue and we understand that some parents do not want their children to have phones or choose for their children to have feature phones that don't allow internet access or app downloads. Decisions about mobile phones and whether children should have them are decisions that should be made by parents. To support parents in making these decisions and to feel more confident about making decisions about the technology their family uses, the school will signpost parents to sources of information including for example parent zone website <https://parentzone.org.uk/>. Our approach to teaching pupils about online safety and how to look after their mental and physical health are outlined above and in our relationships and health education policy

9. Use of social media

In accordance with the PGS Use of ICT Policy, photographs, audio and video recordings of pupils will only be made for official or educational purposes. These may be used within schools as part of displays or training materials and on the school website and Instagram site. Parental consent for this is requested when pupils join the schools and can be withdrawn or changed at any time, with written consent of the parent/carer. Responsibility for the overall content of the school website and school social media sites lies with the headteacher who will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

9.1 Use of social media by staff for personal use.

It is likely that a high proportion of staff will have their own personal social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

- Staff must never add pupils as 'friends' into their personal accounts (including past pupils under the age of 16), nor conduct any communication with a current pupil via a social network site e.g. Facebook, Twitter, WhatsApp, TikTok.
- Staff must not give out their own personal details, such as mobile phone number and personal e-mail address, to pupils.
- Staff are strongly advised not to add parents/carers as 'friends' into their personal accounts.
- Staff must not post comments online about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff must not use social networking sites within the school except for in the staff room during breaks (for personal use). Support staff mobile phones should be kept in the staff room rather than in classrooms or open areas of the school, except with the express permission of SLT for specific reasons relating to urgent communications or safety.
- Staff should ensure that any social networks to which they belong have appropriate levels of security in place to avoid bringing their professional role into disrepute. Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/665520/Teachers_Standards.pdf

or Teaching Assistant Standards <https://www.unison.org.uk/content/uploads/2016/06/Teaching-Assistant-Professional-Standards.pdf>

- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.

- › Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

9.2 Use of social media by parents/carers

This information expands on that covered by the 'Parent Code of Conduct'.

Parents and carers are asked to have regard to their responsibilities in relation to their use of social networking and online comments in any matters related to the school community. Available methods of school communication include the school website, newsletters, emails and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.

Parents should make complaints and raise issues through official school channels rather than posting them on social networking sites. Parents should not post malicious or fabricated comments on social networking sites about any member of the school community. Parents should not share, forward, copy online or on social media/chat groups any details of incidents involving pupils at the school. Such unregulated sharing has the potential to cause great distress for the families concerned.

We understand that some parents/carers use social media - most commonly class WhatsApp groups – to communicate with other parents/carers with children in the same class. The messages in any class WhatsApp groups come from parents/carers in their personal capacity and run independently of the school; the school does not post directly on any WhatsApp parent/carer groups, nor does the school have any administrative responsibility or oversight in these groups. The school communicates with parents through School Ping, emails, the school newsletter and the school website.

The FOPGS communicates through a closed Whatsapp group – this is coordinated by the FOPGS committee and used to organise school events. 'Classlists' is used to sell tickets for events.

We believe it is important to work in partnership with parents/carers to support their child's learning and well-being and create a safe, respectful and inclusive environment for pupils, staff and parents. To help us achieve these aims, we ask that the social media guidelines highlighted below (in bold) are followed by any parents/carers who set up/administer or engage with class WhatsApp groups:

- › **All new groups set up to identify 2-3 administrators and make immediate reference to these social media guidelines**
- › **Class WhatsApp groups should be inclusive and should be open to any parent/carer in the class (the group admin/s are responsible for checking this)**
- › **Groups should never be used as a platform to air views/grievances regarding a child, a parent/carer or a member of school staff**
- › **Content should be relevant and limited to sharing practical matters relating to school and school events i.e. not for private conversations between members**
- › **All communication should be friendly and polite, keeping in mind mutual respect and cultural sensitivity between all members**

Please note, the school considers the following online activity inappropriate:

- › Abusive, malicious or defamatory comments about pupils, other parents/carers, school staff or any member of the school community

- Bringing the school into disrepute

The school takes safeguarding responsibilities seriously and will deal with any reported incidents appropriately.

9.3. Raising Concerns

The school cannot control what is said in WhatsApp groups. We recommend that the Group Administrator of a Class WhatsApp group adheres to these guidelines and ensures that all group members follow them. If a parent/carer has a concern, it should first be raised with the person(s) who have the Group Admin authority.

The school should be alerted if content shared poses a safeguarding risk to a child or if abusive, malicious or defamatory comments have been made about children, parent/carers or staff. If you are concerned about inappropriate comments on a class WhatsApp group, please take a screenshot and contact our senior leadership team by emailing the school office.

9.4 Dealing with incidents of online bullying and inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

If the school is made aware of inappropriate use of social networking, whatsapp groups or online comments by parents which involves any aspect of the school community then the school will communicate with those involved. Depending on the nature of the incident, the school may then:

- Invite those involved into school to meet with a member of the school leadership team
- Contact the appropriate authorities (in cases of criminal behaviour)

Where appropriate the headteacher may refer the issue to the Governing Body who will contact the parent asking them to remove such comments, seek redress through the appropriate channels such as the Complaints Policy.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include, for example, where postings have a racist element or where violence is threatened or encouraged.

10. Filtering and monitoring online activity

The school governors will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The school governors will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The DSL and ICT technicians will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

Deliberate breaches of the filtering system will be reported to the DSL who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, the school will respond in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the School Disciplinary Procedure. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored.

Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy and Procedures.

11. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Staff members will be responsible for keeping their passwords private. Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

12. Emails

Access to and the use of school emails will be managed in line with the Data Protection Policy and the Acceptable use of ICT and Data Agreement.

Staff will be given approved school email accounts and will only be able to use these when doing school-related work. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable use of ICT and Data Agreement. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Parents should contact staff via the school admin email address. In general, staff will keep responses to parent emails brief and arrange a phone call or a meeting to discuss any concerns. Staff members will be required to block spam, junk and phishing mail. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. The senior leadership team provide annual updates to staff which include information on the following:

- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

13. Training for staff, governors and volunteers

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).

The DSL and Deputy DSLs 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.

14. Monitoring arrangements

This policy will be reviewed annually and approved by the governors This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links with other policies

This online safety policy is linked to our:

- › Child protection and safeguarding policy
- › Behaviour policy
- › Staff disciplinary procedures
- › Data protection policy and privacy notices
- › Complaints procedure
- › Acceptable use of ICT policy
- › Code of conduct (Staff and Parent)

