Online Safety Policy

SAFEGUARDING & WELLBEING

Date	Review Date	Coordinator	Nominated Governor	Approved
April 24	April 25	M Ajayi/T Coceal		13.05.24

Contents

Aims

- To provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- 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')
- To raise educational standards and promote pupil achievement.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- To ensure compliance with all relevant legislation connected to this policy.
- To work with other schools and the local authority to share good practice in order to improve this policy.
- 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:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
2. **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
3. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing other explicit images and online bullying; and
4. **Commerce** – risks such as inappropriate advertising, phishing and/or financial scams

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 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. We work closely with the School Council to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

Responsibility of the Policy and Procedure

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 coordinate regular meetings with appropriate staff to discuss online safety and requirements for training.

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 filtering and monitoring standards, and discuss with IT staff and service providers 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 their safeguarding needs.

The governor who oversees online safety is Attiyah Khan (Safeguarding Governor).

All governors will:

- Ensure 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 (see Acceptable Use Policy)
- 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

The Headteacher

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

The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions.
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 Computing Lead 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
- Working with the Computing Lead to make sure the appropriate systems and processes are in place
- Working with the Computing Lead 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
- Ensuring that any online safety incidents are logged (on CPOMs) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged 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
- Undertaking annual risk assessments, with the Computing Lead, that consider and reflect the risks children face
- 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

This list is not intended to be exhaustive.

The Computing Lead/School Personnel

The Computing Lead 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 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 [weekly/fortnightly/monthly] basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

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, and ensuring that pupils follow the school's terms on acceptable use (see Acceptable User Policy)
- 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 by following the school's reporting procedure (see the school's Safeguarding and Child Protection Policy)
- 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'
- All users are responsible for the security of their username and password and must not allow other users to use this information to access the system. All breaches of security must be reported

This list is not intended to be exhaustive.

Parents/Carers

Parents/carers 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 (see Acceptable User Policy)
- be aware of and comply with this policy;
- make their children aware of the Online-Safety policy;
- be encouraged to take an active role in the life of the school by attending:
    - parent open evenings
    - parent-teacher consultations
    - class assemblies
    - school concerts
    - fundraising and social events

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
- Hot topics – Childnet
- Parent resource sheet – Childnet

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 (see Acceptable User Policy).

Role of Pupils

Pupils will be aware of this policy and will be taught to:

- be critically aware of the materials they read;
- validate information before accepting its accuracy;
- acknowledge the source of information used;
- use the Internet for research;
- respect copyright when using Internet material in their own work;
- report any offensive email;
- report any unsuitable website or material to their teacher who will liaise with the Online Safety Manager;
- know and understand the school policy on the use of:
  - mobile phones
  - digital cameras
  - handheld devices
- know and understand the school policy on the taking and use of photographic images and cyberbullying;
- listen carefully to all instructions given by the teacher;
- ask for further help if they do not understand;
- treat others, their work and equipment with respect.

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the National Curriculum computing programmes of study. We have also made links to the government's guidance on relationships education and health education.

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

Educating Parents/Carers about Online Safety

The school will raise parents/carers' awareness of internet safety in the newsletter 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' evenings.
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 (who is also the DSL).
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber Bullying

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.
Please see the school's Behaviour and Anti Bullying Policy for further information.

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 (see Internet and E-mail Acceptable Use Policy). 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 (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

Pupils using Mobile Devices in School

Mobile phones or devices are not permitted in school by pupils from Reception to Year 4. It is a requirement that all pupils in these year groups are collected from school by a responsible adult and therefore the need for a child of these ages to make telephone contact will not arise.
While we fully acknowledge a parent's right to allow their child (in Years 5 or 6) to bring a mobile phone to school if they walk to and from school without adult supervision, we discourage pupils

from bringing mobile phones to school due to the potential issues raised above.

Pupils in Years 5 and 6 can only bring a mobile phone into school on the understanding that:

- the mobile phone is not used on the school site, including at either end of the school day
- parents inform the school that their child has a mobile phone and a permission slip (Appendix 1) must be signed by the parent/ carer
- the mobile is handed to the school office on arrival and collected at the end of the day before leaving the school
- phones are clearly marked so that each pupil knows their own phone
- parents should talk to their children about the inappropriate use of text messages as they can often be used to bully pupils.

If a pupil is found by a member of staff to be using a mobile phone, the phone will be confiscated from the pupil, handed to a member of the office team who will record the name of the pupil and attach it to the phone. The mobile phone will be stored by the school office. The pupil may collect the phone at the end of the school day. A letter will be sent home to parents requesting that a permission slip be returned the next day. If this practice continues on more than three occasions, then the school will confiscate the phone until an appropriate adult collects the phone from a senior teacher.

Please refer to the school's Mobile Phone/Device Policy for more information.

Staff using Work Devices outside of 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 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 for a period of time
- Not sharing the device among family or friends
- Staff members must not use the device in any way that would violate the school's terms of acceptable use (see Acceptable User 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 Headteacher, Computing Lead or ICT Technician.

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, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent 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 deputy/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.

Filtering and Monitoring

Filtering

- We have a contract with a reputed and national Internet provider to manage a secure and filtered Internet service, enabling us to safely access and use the Internet and all email. The Internet filtering service will be reviewed annually
- All users access the Internet in accordance with the School's Acceptable User Agreement and will inform the Designated Safeguarding Lead and Online Safety Manager if at any time they find they have accessed inappropriate Internet sites
- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges, and the guidance provided in the UK Safer Internet Centre Appropriate filtering
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police-assessed list of unlawful terrorist content produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective

- there is a clear process to deal with and log requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

Monitoring

- The school has monitoring systems in place to protect the school systems and has third-party software installed on all devices used by pupils to monitor ICT use across the school.
- The Designated Safeguarding Lead urgently picks up monitoring reports, acts on them, and
  records outcomes. All users are aware that the network (and devices) are monitored.
- Effective protocols are in place to report abuse/misuse. There is a clear process for prioritising responses to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:
    - physical monitoring (adult supervision in the classroom)
    - internet use is logged, regularly monitored and reviewed
    - filtering logs are regularly analysed and breaches are reported to senior leaders
    - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
    - where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
    - use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).

When inappropriate material has been accessed, school safeguarding procedures will apply (see Safeguarding Policy).

School Website

Contact details on the website will be:

- the school address
- e-mail address
- telephone number

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

Social Media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.
All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use:

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the

scope of this policy

- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours

Monitoring of Public Social Media

As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.

The school should effectively respond to social media comments made by others according to a defined policy or process.

When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Links with Other Policies

- Safeguarding and Child Protection
- Safeguarding: Pupil Version
- Acceptable Use and Agreement
- Behaviour and Anti Bullying
- Code of Conduct
- Mobile Phone/Device
- Social Media
- Data Protection
- Internet and E-mail Acceptable Use Policy for Foxdell Primary School employees
- Personal, Social, Health Education (PSHE) Policy including Relationships Education and Health Education (RHE)