Online Safety Policy

Last Reviewed	**November 2022**
Review date	**November 2024**
K. Pochin **Headteacher**	**Rob Johnson** **Chair of Governors**

Contents

Introduction & Aims

This Online Safety Policy outlines the commitment of Inglehurst Infant School to safeguard members of our school community online in accordance with statutory guidelines and best practice.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school.

It also applies to the use of personal digital technology on the school site (where allowed).

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Outline robust processes to ensure the online safety of pupils, staff, volunteers and governors
- Prevent the disruption of school through the misuse of, or attempted misuse of ICT related systems
- Is made available to staff at induction and through normal communication channels
- Is published on the school website.

Roles and responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

The Headteacher and DSL

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

Details of the school's DSLs are set out in our child protection and safeguarding policy and displayed around school.

The deputy DSL's will support the head teacher and DSL in implementing this policy.

The Headteacher who is our school's 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, the ICT manager and other staff, as necessary, to address any online safety issues or incidents and ensure robust monitoring and filtering systems are in place.
- Ensuring that any online safety incidents are reported to the DSL or deputy DSLs and dealt with appropriately in line with this policy and other school policies such as the Safeguarding Policy and Behaviour Policy.
- Updating and delivering staff training on online safety through whole school training sessions and briefing sheets throughout the year. Liaising with other agencies and/or external services if necessary.

The Headteacher/DSL is aware of the following:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying

Curriculum Leads

Curriculum leads will work with the headteacher to develop a planned and coordinated online safety education programme

This will be provided through:

- ICT curriculum
- Assemblies
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- Age appropriate pupils online rules

All staff and volunteers

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

- Maintaining an understanding of this policy and implementing it consistently throughout the curriculum and other school activities.
- 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 rules
- Working with the DSL and deputy DSL's to ensure that any online safety incidents are reported, logged and dealt with appropriately in line with this policy
- Having a zero-tolerance approach to incidents of cyber-bullying, sexual harassment, discrimination etc both online and offline and maintaining an attitude of 'it could happen here'.
- Ensure that any incidents are reported and dealt with in line with the school's behaviour safeguarding procedures. both online and offline and maintaining an attitude of 'it could happen here'
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Governors

The Governors are responsible for the approval of the online Safety Policy and for reviewing the effective of the policy.

The Governors should be advised of any online safety incidents and ensure that staff training is in place and incorporates up to date online safety education.

Ensure that through discussions with the Headteacher and subject leaders' online safety is embedded within the curriculum.

System management responsibilities

The school in conjunction with the ICT support provider and ICT technician, will be responsible for ensuring that their infrastructure/network is a safe and secure as is reasonably possible and that procedures set out within this policy are implemented.

- Ensure that the school meets the minimum requirements for online safety as identified by the local authority/MAT or other relevant body.
- Monitoring and filtering systems will be regularly monitored and reviewed and any concerns reported to the head teacher. These systems will be regularly updated to keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist

- Ensuring that the school's ICT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly

Blocking access to potentially dangerous sites and where possible, preventing the downloading of potentially dangerous files

Technical staff should be aware of and operate in accordance with all relevant school policies.

All members of staff and governors are provided with a school email address. Electronic communications with students, parents/carers and other professionals will only take place via work-approved communication channels e.g. via a school-provided email address, Class Dojo or a school telephone number. Staff are advised to ensure that business correspondence is received to and sent from the school email address. This is to protect staff's privacy and ensure that school business is kept separate from private correspondence.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child is supervised when using the internet at home.

Educating and supporting Parents

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

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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

Educating pupils about online safety

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

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

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

Cyber-bullying

Definition

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

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.

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

Pupils using mobile devices in school

Pupils are not permitted to bring mobile devices into school. If it is discovered that a pupil has brought a mobile device into school a member of staff will take it to the school office to be locked away for safe-keeping and parents or carers will be informed to make arrangements to collect it.

Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords 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 device is used for professional use only
- Not sharing the device among family or friends
- Keeping operating systems up to date – always allow the device to automatically install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use,

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 Head teacher.

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 policies on Acceptable Internet Use. 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 our staff disciplinary procedures/staff 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.

Training

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. Key messages are then disseminated with staff.

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

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).

Volunteers will receive appropriate training and updates, if applicable.

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

Monitoring arrangements

The DSL and Deputy DSL's will monitor behaviour and safeguarding issues and logs related to online safety. This policy will be reviewed every two years by the headteacher. At every review, the policy will be shared with the governing body.

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
- ICT and internet acceptable use policy
- VPN & Staff laptop agreement policy
- Staff Acceptable Internet Use Policy (AIUP)
- Acceptable Use Policy AUP