+ We can do everything together, loving and learning through God +

Ingrave Johnstone Church of England Primary School

e-Safety and Pupil Acceptable Use Policy

Agreed by Governors: Spring 2024

Review Date: Spring 2027

e-SAFETY POLICY

At Ingrave Johnstone C of E Primary School we create a secure and safe environment that encourages communication, self belief, mutual respect and success. We provide a rich and balanced curriculum that develops every child, allowing them to achieve their true potential.

Our school recognises e-safety issues and the potential harm and risks it can pose to children and young people. All partner agencies, stakeholders, schools and educational settings and all other organisations within the community providing services to children have a duty to understand e-safety issues as part of its wider safeguarding duties; recognising their role in helping children to remain safe online while also supporting the adults who care for children.

This policy is based on the Department for Education (DFE's) statutory safeguarding guidance: Keeping Children Safe in Education Document Annex C, and its advice for schools about: Teaching Online Safety in Schools, Preventing and Tackling Bullying, Cyber-Bullying. Advice for Headteachers and School Staff, Searching, Screening and Confiscation and advice published by the UK Council for Online Safety. It should also be read in conjunction with the school's Behaviour Policy, Child Protection Policy, Anti-bullying Policy and Harmful Sexual Behaviour Policy.

Aims

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Filters and Monitoring

Ingrave Johnstone C of E Primary school uses filtering and monitoring systems that are supplied with the broadband service provided by RRA Services. This system regularly monitors the traffic on the network and the use of certain websites and search topics are restricted. The designated safeguarding lead is alerted if any concerns are raised through filtering and monitoring reports, which are monitored weekly by our IT Technician and will deal with any incidents in line with our existing safeguarding and child protection polices and procedures.

Information and Support for Parent, Staff and Governors

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, letters, newsletters, website updates, and information about e-safety campaigns.

Roles and Responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). 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;
- 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

- The DSL takes lead responsibility for online safety in school, in particular;
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the headteacher, IT technician and other staff, as necessary, to address any online safety issues or incidents;
- Managing all online safety issues and incidents in line with the school child protection policy;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour and anti-bullying policies;

- Updating and delivering staff training on online safety;
- 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. This list is not intended to be exhaustive.

The IT Technician

The IT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's IT 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 IT systems on a monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged 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 and anti-bullying policies.

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 of the school's Acceptable Use Policy with regard to appropriate use;
- Working with the DSL to ensure that any online safety incidents are logged 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 and anti-bullying policies;
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Understand that their child has read, understood and agreed to the terms of the school's Acceptable Use Policy (Appendix 1). 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 International
- Parent resource sheet – Childnet International

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 of the Appropriate Use Policy.

Teaching of Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

• A planned e-safety programme will be provided as part of the Computing Curriculum;

• Key e-safety messages are reinforced as part of a planned programme of assemblies and activities;

• Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;

• Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;

• Through the promotion of British Values and the Prevent Duty the pupils will be taught to challenge extremist views when using material accessed on the internet;

• Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

From the National 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.

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. The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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. (See also the school's Behaviour and Anti-bullying Policies).

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.

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 cyberbullying, its impact and ways to support pupils, as part of safeguarding training.

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

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

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

Examining Electronic Devices – Searching Screening and Confiscation

The school will follow guidance from Searching, Screening and Confiscation DfE 2022, UKCIS guidance and school's Behaviour Policy 2022.

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

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;
- Making sure the device locks if left inactive for a period of time;

- Not sharing the device among family or friends;
- Installing anti-virus and anti-spyware software;
- Keeping operating systems up to date by always installing the latest updates.

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

Work devices must be used solely for work activities.

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

Data Protection

In line with the school's Data Protection Policy, all staff and governors must be aware of the risks posed by data being accessed by unauthorised people. All members of staff and governors must take appropriate steps to minimise this risk by ensuring that all data is kept on password encrypted memory sticks and disposed hard drives are securely destroyed by registered companies when no longer required.

Further information can be found on the following websites:

www.ceop.gov.uk

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

http://educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation

www.gov.uk/UKCCIS

Appendix 1

Primary Pupil Acceptable Use

Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

eSAFETY

ICT including the internet, e-mail and mobile technologies etc, has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss the eSafety rules attached with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact your child's class teacher.

This Acceptable Use Agreement is included in our eSafety and Data Security Policy.

***e*SAFETY**

We have discussed this and .....(Child's Name) of Class..... agrees to follow the eSafety rules and to support the safe use of ICT at Ingrave Johnstone C of E Primary School.

Signed..... Parent/Guardian

Date.....

Ingrave Johnstone C of E Primary School fully complies with information legislation. For the full details on how we use your personal information please see the Privacy Notice in the Data Protection/GDPR section on our website or call 01277 810218 if you are unable to access the internet.