CROSSENS NURSERY SCHOOL - E Safety Policy (reviewed in line with KCSIE 2023)

Crossens Nursery School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communication technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Crossens Nursery School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be once a year or whenever it is updated
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information at parents evenings and through the school newsletter

Roles and Responsibilities

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 co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 those 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 Sarah Howard.

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
- 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 and deputies

Details of the school's designated safeguarding lead (DSL) [and 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:

- Supporting the headteacher in ensuring 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 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 ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager 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 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 policy
- 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
- Undertaking annual risk assessments 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 ICT manager

The ICT manager 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 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 Our Caring Crossens policy

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
- 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 recording any online safety incidents onto the 'Online Safety Incidents Form' and reporting this to the DSL who will action accordingly with Schools Broadband.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with Our Caring Crossens 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'
- Reading and understanding the Schools Broadband guidance on filtering, included in the appendices of this policy

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

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 on acceptable use.

Physical Environment/Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly.

- Anti-virus software is installed on all computers and updated regularly

- All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the Headteacher. All incidents will be recorded in the Incident other than Accident log for audit purposes.
- Pupil use of the internet is monitored by all staff
- Staff use is monitored by the IT technician and reported to the Headteacher
- All staff are issued with their own username and password for network access.

Filtering and Monitoring

Our filtering system is provided by Schools Broadband under the name 'Netsweeper'. All pupil facing devices have the maximum filtering. All devices have an up to date windows defender that give protection against viruses and provides a device level firewall. We also have a Firewall that blocks unwanted traffic inbound on the router and this is also provided by Schools Broadband. For further information, please see the guidance from Schools Broadband in the appendices of this policy.

Mobile / emerging technologies

- Nominated teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
- To ensure the security of the school systems, only authorised personal equipment is permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with school policy.
- Pictures /videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community
- Personal mobile phones/ devices are not to be taken in to the classroom

E-mail

The school e-mail system is provided by Schools Broadband.

- Nominated staff are given a school e-mail address and understand that this must be used for all professional communication
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Staff are not allowed to access personal e-mail accounts on the school system.
- Everyone in the school community understands that any inappropriate e-mails must be reported to the Headteacher as soon as possible
- If accessing emails from home, staff understand that other family members must not have access to this private and confidential information

Published content

The Headteacher takes responsibility for content published to the school web site.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses
- The school does not publish any contact details for the pupils

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Students' full names will not be published outside the school environment
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 2018.

The school is registered with ICO for this purpose.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Schools Broadband Service Desk will also be informed.
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the DSL
- Breaches of this policy by staff will be investigated by the Headteacher. Action will be taken under the schools Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
- The Educations and Inspections Act 2006 grants the Head Teacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

Policy Reviewed September 2023

To be reviewed September 2025

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**