High Ercall Primary School

E-Safety Policy

Date of Policy Creation	**September 2020**	**Named Responsibility**	Gemma Lingham
Date of review completion	**September 2021**	**Named Responsibility**	Gemma Lingham
Inception of new Policy	**September 2021**	**Named Responsibility**	Sarah Roberts
Date of Policy Adoption by Governing Body			

HIGH ERCALL PRIMARY SCHOOL CURRICULUM POLICY GUIDANCE FOR E-SAFETY

RELATED POLICIES AND PROCEDURES THIS POLICY STATEMENT SHOULD BE READ ALONGSIDE OUR ORGANISATIONAL POLICIES AND PROCEDURES, INCLUDING:

- CHILD PROTECTION
- PROCEDURES FOR RESPONDING TO CONCERNS ABOUT A CHILD OR YOUNG PERSON'S WELLBEING
- DEALING WITH ALLEGATIONS OF ABUSE MADE AGAINST A CHILD OR YOUNG PERSON
- MANAGING ALLEGATIONS AGAINST STAFF AND VOLUNTEERS
- CODE OF CONDUCT FOR STAFF AND VOLUNTEERS
- ANTI-BULLYING POLICY AND PROCEDURES
- PHOTOGRAPHY AND IMAGE SHARING GUIDANCE

INTRODUCTION AND SUBJECT DEFINITION

E-safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and potential risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

High Ercall Primary School has a whole school approach to the safe use of digital technology and creating this safe learning environment includes three main elements: - a robust provision of network and internet security (provided by Telford and Wrekin Council) - policies and procedures with clear roles and responsibilities and a comprehensive e-safety programme for pupils, staff and parents.

Why Is Internet Use Important?

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business, and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and High Ercall has a duty to provide pupils with quality internet access. Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security. At High Ercall, students learn how to conduct themselves respectfully online and keep themselves and others safe.

E-SAFETY CURRICULUM

Risks of internet use

When planning an effective programme of study for e-safety it is important to consider the potential risks. The breadth of issues classified within online safety is considerable, but can be categorised into four 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;
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying; and
- commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams.

High Ercall School ensure our E-safety curriculum is robust and carefully considers the safeguarding implications the online world poses. We recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.

Skills and Expectations

High Ercall has a clear, progressive e-safety education programme as part of the computing curriculum and PSHE curriculum. It is built on LA and E-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- (for older pupils) To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour, keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post photos or videos of others without their permission.
- To know not to download any files, such as music files, without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- (for older pupils) To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting, and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

Our Aims

At High Ercall, we:

- Ensure that all children read and sign the Acceptable Use Agreement in school. A copy of this is displayed in the classroom and is used as a point of reference. Parents can access this on the school website???
- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Use Thinkuknow, Project Evolve, Be Internet Legends and PSHE association to inform our e-safety planning.
- Ensure staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright / intellectual property rights.
- Ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in popups, buying on-line, on-line gaming / gambling. If we feel our pupils, students or staff are at risk, this will be reported to the Anti-Phishing Working Group.
- Ensure parents are aware of e-safety safeguarding issues – both locally and nationally - through the use of the school weekly newsletter and parent workshops.

Responsibilities of staff

- All staff will be aware of systems within High Ercall School which support safeguarding and these will be explained to new staff as part of their induction, this will include the measures to prevent cyberbullying.
- All staff receive appropriate safeguarding and child protection training (including online safety) at induction. This training will be updated through regular staff meetings to provide them with relevant skills and knowledge to safeguard children effectively.
- All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life.
- All staff will be aware of peer on peer abuse and that this can occur online, this can take the form of abusive, harassing and misogynistic messages, the non-consensually sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.
- In all cases, if staff are unsure, they should always speak to the Designated Safeguarding Lead (DSL) or deputies.

Responsibilities of the governing body

Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including online safety and the requirement to ensure children are taught about safeguarding, including online safety, that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.

The governing body should be doing all that they reasonably can to limit children's exposure to the risks from the school's IT system. As part of this process, the governing body should ensure the school has appropriate filters and monitoring systems in place. They should consider the age of our pupils, how many pupils are in school, how often IT systems are accessed and the costs versus risks. However, care should also be taken that filters and monitoring systems do not place unreasonable restrictions on what children can be taught about online safety.

Covid-19

During the Covid-19 pandemic, online learning has featured hugely in our curriculum both in school and remotely through home learning. High Ercall School have:

- Ensured that computing lessons during Term 1 Autumn 2020 are dedicated to E-safety.
- Used PSHE lessons to further embed this learning.
- Featured online safety announcements, guidance and advice on the weekly newsletter.
- Ensured home learning contains a minimum of one E-safety awareness task.
- Taken advice from UK Safer Internet Centre guidance on safe remote learning
- Continued to follow the child protection/safeguarding policy when reporting any safeguarding concerns.
- Updated the E-safety policy and reviewed the 360 safe self-review tool.

Managing Internet Access

The internet is an open communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas, and publish material, which makes it both an invaluable resource for education as well as a potential risk to young people.

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.

- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to senior management. The unsuitable site must be reported to the internet provider (Telford and Wrekin Council) so it can be blocked. An incident like this should also be logged in the schools safeguarding and behaviour system (CPOMS).
- Children should only use messaging software if the teacher has allowed it and it is for educational purposes in a safe environment.
- Videos should be screened first by staff before being shown to children in lessons.
- Children can search for videos and images for educational purposes, but this must be done in a controlled environment.
- Internet filtering is managed by our internet and network provider, Telford and Wrekin Council.
- Anti-virus management is controlled and monitored by our internet and network provider, Telford and Wrekin Council.
- Acceptable use of the internet is monitored by online safety lead using SENSO and a log is kept of inappropriate use. Action is taken according to the behaviour policy and recorded on CPOMS.

Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

- Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.
- Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.
- Staff agree and sign an Acceptable Use Agreement at the start of the academic year that includes the use of mobile phones and other devices.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords.
- We require staff to change their passwords every 90 days.
- Each class have a Username and Password that changes every term.
- Pupils are taught what constitutes a strong password as part of their computing curriculum.

MONITORING AND INCIDENT HANDLING

At High Ercall there is strict monitoring and application of the E-safety policy and a differentiated and appropriate range of sanctions, though it is extremely rare that sanctions are needed.

- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- On discovery of an e-safety incident, the E-safety Coordinator is informed and they work with the DSL to review the information and conduct a thorough investigation. This could include: evaluating the offending content online; talking to the class teacher, support staff and the child/children or using SENSO (our online monitoring system) to gain insight into the incident.
- Support is actively sought from other agencies as needed (e.g. the local authority, IT support, UK Safer Internet Centre helpline, police) in dealing with e-safety issues.

- Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA. The Computing/E-safety Coordinator and Head Teacher keep the records of e-safety incidents.
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Any safeguarding incidents are reported to Designated Safeguarding Lead (DSL) Mrs Roberts or to Mr Parton (Deputy Safeguarding Lead)

REVIEW AND MONITORING

- The E-safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education policy and in the School Development Plan.
- The school has an E-safety and Computing Coordinator who will be responsible for document ownership, review, and updates.
- The E-safety Policy will be reviewed annually or when any significant changes occur regarding the technologies in use within the school.
- The E-safety policy has been written by the school E-safety and Computing Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school E-safety policy will be discussed in detail with all members of teaching staff.
- We use an online safety self-review tool, 360 safe, to review and monitor our e-safety policy and procedure. This is reviewed annually to ensure we are up to date with this rapidly changing area.

PROFESSIONAL DEVELOPMENT

All staff have undertaken GDPR, safeguarding and e-safety training and have the opportunity to partake in extra training to further their professional development. All staff sign an Acceptable Use Agreement at the start of each academic year. This can be found on our website or parents can request a hard copy from the school office.