Greenside Primary School

Online Safety Policy

Last reviewed: March 2021
To be reviewed: March 2022
Written by: Rebecca Winkley
Ratified by the Governors on: 11th March 2021

Greenside Online Safety Policy

Introduction
Online safety encompasses all internet technologies and electronic communications such as mobile phones and tablets. The increased use of these technologies highlights the need for children to be educated about their risks and benefits and provides safeguards and awareness for children to be able to control their online experience. Online safety is a safeguarding issue not an ICT or Computing issue and all members of the school community have a duty to always be aware of online safety, to know the required procedures and to act on them. This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements. The purpose of internet use in School is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the School's management information and business administration systems. This policy complements and supports other relevant School and Local Authority policies. This policy is based on the Department for Education's (DfE) 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 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. The policy also considers the National Curriculum computing programmes of study.
Roles & Responsibility
The Headteacher or, in her absence, the Deputy Headteacher or Assistant Headteacher, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care. 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) 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 ICT manager and other staff, as necessary, to address any online safety issues or incidents
- 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, organising and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- 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 policy

Ethos

It is the duty of the School to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the 'Every Child Matters' agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the School's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the School and its everyday practice and procedures. All staff have a responsibility to support safe practices in the use of technology.

Our school aims to:

- 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Educating Pupils about Online Safety

Why Internet use is important

The internet is an essential element for education, business and social interaction. The school offers provision to pupils to access the internet as part of their learning experience. It is also a resource for both staff and pupils.

The text below is taken from the National Curriculum computing programmes of study.

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Benefits of Internet Use for Education

The internet is part of the statutory curriculum and as such, is a necessary tool for staff and children. It allows access to worldwide educational resources and become active participants in a digital world.

Internet use will enhance learning

- The school internet access is designed for pupils and will include appropriate filtering
- Pupils will be taught about acceptable internet use and will be given clear objectives for this
- Pupils will be taught effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught how to evaluate Internet content
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

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 one person or group by another person or group, where the relationship involves an imbalance of power.

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.

The school will publish information/leaflets on the school website about 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.

Managing Internet Safety

Information system security

School ICT systems capacity and security are reviewed regularly. All internet access is filtered by the school's ISP (Internet Service Provider) and we will work together with them to ensure the efficacy of the filter as far as practicably possible. We recognise that no filter can ever be perfect, therefore, children will be taught the necessary skills to manage risks themselves on an age appropriate level. Virus protection is updated continuously and a full scan is run daily.

Published content and the school website

The contact details on the school website should only include the school's e-mail address, address and telephone number. Staff e-mail addresses will not be published. The Headteacher will take overall responsibility for checking the accuracy and appropriateness of the content of the website.

Publishing pupils' images and work

Written permission will be obtained from Parents/Carers on entry, before photographs of children are placed up on the school website or any social media. Pupil's full names will not be used on the school website, particularly in association with photographs.

- The School Network blocks/filters access from most social networking sites.
- Despite this, we will educate children on the safe use of these technologies as we are aware that our learners may choose to access these resources outside of school.
- Newsgroups are blocked unless a specific use is approved.
- Pupils will be advised never to give out any personal details which may identify them or their location.
- Pupils and parents will be advised that use of social networking sites outside of school is inappropriate for primary aged pupils, and further information will be provided to parents regarding this.

Managing Filtering

The school will work with Schools Broadband (or any future ISP) to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover an inappropriate website it must be reported to the designated safeguarding lead. The network manager, alongside staff, will ensure that regular checks are made to ensure that the filtering methods selected are effective, appropriate and reasonable. Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies (behaviour and ICT and internet acceptable 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 system or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the 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.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and children will be supervised and monitored when using these.
- Mobile phones are not to be used during school hours. The sending of abusive or inappropriate text messages is strictly forbidden. Pupils must not bring mobile phones into school and if they do, the phone must be switched off and stored securely in the school office until the end of the school day.
- Children will be educated about the risks inherent in the use of social messaging apps as we are aware that they may use these when outside of school.
- Staff will be issued with a school phone if contact with pupils or parents is required.

Managing data security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2018.

Policy decisions

- All staff and governors must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school will keep a record of all staff/pupils who are denied internet access. The record will be kept up to date.
- In Key Stage 1, access to the internet will be under direct supervision, with access to approved online materials. In Key Stage 2, pupils will be supervised a group when using the internet.
- Parents/Pupils will be asked to sign and return a consent form on their child's behalf when starting school to enable children to access the internet in school, this will outline the need to remain safe online and follow schools acceptable use policy.

Assessing risks

The school will take all reasonable precautions to ensure that users only access appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Schools Broadband can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.

The school will audit ICT provision to ensure that its content is appropriate and its implementation effective.

Handling Online safety complaints

- Complaints of Internet misuse and/or Online safety will be dealt with by the school's designated safeguarding lead.
- Any complaint over staff misuse should be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance to school child protection procedures.
- Responses to internet misuse will include informing parents/carers of the incident.
- Further sanctions may include the removal of internet/computer access for a period of time.

Communications Policy

Introducing the Online safety policy to Pupils

- Acceptable use posters will be positioned in all rooms where computers are used and discussed with pupils throughout the school year. All pupils will sign a pledge outlining the rules of Online Safety, displayed in each classroom.
- Pupils will be informed that Internet use will be monitored.
- Regular online safety lessons and/or assemblies will be given; including through the celebration of Safer Internet Day.

Staff and the Online safety policy

- All staff will be shown where the Online safety policy is found on the shared staff network and its importance explained.
- Staff will be aware that Internet use can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will receive child protection and Online Safety training regularly

Enlisting parental support

- Parents' attention will be drawn to the school's Online safety policy in newsletters and on the school website.
- A partnership approach will be encouraged, through use of parent ICT evenings and information on safe home Internet use.