

Greenfields Community School



E-Safety Policy

DOCUMENT PROVENANCE			
Status	Draft	Current version no.	1.0
Organisation	NCC/NST	Version date	September 2023
Audience	Anyone	Approval date	
Security classification	OFFICIAL	Next review date	Annually

DOCUMENT CHANGE HISTORY			
Revision date	Version no.	Author of changes	Summary of changes
December 2022	2	Terry Smith	Update
September 2023	3	Terry Smith	Update
September 2024	4	Lou Maltby	Update

GREENFIELDS COMMUNITY SCHOOL

Reviewed September 2024

E-SAFETY POLICY

1. Aims

Greenfields Community School aims to provide the children with a computing curriculum that develops them as safe internet users. We aim to provide a stimulating learning experience, through all subjects and the creative curriculum.

2. Rationale

2.0 The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using Computing. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed, Computing is an essential life-skill.

2.1 E-safety will be incorporated into the Computing and RSHE/SMSC curriculum.

2.2 Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

3. Internet Use

3.0 How will pupils learn 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

4. Managing information

4.0 How should published website content be managed?

- The Computing Leader & Senior Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

4.1 Can pupil's images or work be published?

- Parents are asked to sign consent for pupil's images to be published on the school website during their child's admission.
- Pupil names will only be used by permission
- Pupil work can only be published with their permission.

4.2 How will social networking, social media and personal publishing be managed?

- Pupils and staff will not be allowed access to public or unregulated chat rooms and social networks during school time.
- The school will BLOCK access to social media and social networking sites.
- During e-safety assemblies, Computing and PSHE lessons, pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Teachers will follow the DfE Teachers' Standards

5. Internet Access

5.0 How will Internet access be authorised?

- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents and pupils will be asked to read and sign a user agreement.
- Children will only have access to the internet under supervision from an adult.

5.1 How will the risks be assessed?

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly through the governors.
- The headteacher and governors will ensure that the Internet policy is implemented and compliance with the policy monitored.

5.2 How will filtering be managed?

- The COMPUTING Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- The school will use the NCS (Net Sweeper) filtering system on the broadband connection and 'allow lists' restricting access to a list of approved sites.
- The school will work in partnership with Schools IT to ensure systems to protect pupils are reviewed and monitored.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Computing Leader/Technician/Headteacher
- Any material that the school believes is illegal must be referred to the CEOP and/or Internet Watch Foundation.
- Any member of staff, may contact Professionals online safety helpline 0844 3814772 for advice on any e-safety incident

5.3 How will Cyber bullying be managed?

Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence (copies of offensive messages or screen shots).

The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyber bullying include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Access to school systems will be blocked
- Parent/Carers will be informed.
- The Police will be contacted if a criminal offence is suspected.

6. Communications

6.0 How will the policy be introduced to pupils & parents?

- Rules for Internet access will be posted in all rooms where computers are used.
- Parents and Pupils will agree to the schools Acceptable Use Policy in September.
- Pupils will be informed that Internet use will be monitored.

- Instruction in responsible and safe use should precede Internet access.
- Assemblies about e-safety and Participation in Safer Internet Day organised nationally.
- The school website will contain a page advising parents of ways for their children to Stay Safe online .

6.1 How will staff be consulted?

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school. During recruitment new staff must read and sign the Code of Conduct.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the E-safety and Internet Policy, and its importance explained.
- All staff should closely monitor internet use within their classroom.
- All staff report any E-safety incidents in the Internet Safety Incident Reporting Log.

7. Monitoring

This policy, e-safety procedures and e-safety incidents will be monitored by the Head Teacher and Governors. Please see Governing body terms of reference.

Our Internet Policy has been written by the school, building on the Kent County Council SEGfL e-safety policy and government guidance. It has been approved by governors.

PLEASE ALSO SEE THE GREENFIELDS COMMUNITY SCHOOL FILTERING AND MONITORING POLICY

Date: September 2024

To be revised: September 2025