

Anston Greenlands Primary School



ONLINE SAFETY POLICY

Summer Term 2022

Headteacher: Mr A Wirth
Edinburgh Drive
North Anston
Sheffield S25 4HD
Tel: 01909 550557
Email: office@greenlandsprimary.org
www.anstongreenlands.org



Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Managing Safe Internet Access

- All school staff have a shared responsibility for online safety.
- Assemblies, PSHE lessons and ICT lessons can be used to help pupils to become safe and responsible users of new technologies.
- An age-related curriculum for the teaching of online safety has been developed. Use will be made of anti-bullying week and/or Safer Internet Day to highlight online safety.
- While discrete lessons are useful, internet safety concepts should be embedded within the curriculum wherever possible, while safety messages should be reinforced every time pupils use the internet and related technologies.

Risks linked to the use of the internet:

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

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Children will be taught about how to manage the risk (both to themselves and others) linked to these three areas.

Technology use and online safety issues go hand in hand. Many incidents happen beyond the physical geography of the school and yet can impact on pupils or staff.

Safe Internet use to enhance learning

- The school Internet access is provided by 'Impelling'. It is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- As part of ICT and cross curricular lessons, pupils are taught about the Internet use that is acceptable and what is not and given clear objectives for Internet use.
- A set of online safety rules has been developed, with input from pupils and staff. This will be reviewed regularly.
- A Student Leader group called the 'ICT Cadets' is well established. This comprises Y4, 5 and 6 students; it is run by an HLTA with support from teachers, as required. The group promotes online safety across school and within the local community. An action plan is created by the ICT Cadets at the beginning of each school year.

- All pupils will be asked to read, agree and sign an age-appropriate Acceptable Use Agreement at the beginning of each year. This will be displayed in all classrooms and on the school website. The 'ICT Cadets' group will ensure that the Acceptable Use Agreement is up-to-date and uses child-friendly language.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content when they are not in school.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.

Information system security

- The school ICT systems' security will be reviewed regularly.
- Virus protection is provided through 'Impelling'.
- If children wish to send homework electronically to school, this should be done by emailing the school email address of the staff member involved. Pupils' memory sticks and CD Roms should not be used in any of the school computers.
- All laptops which may be taken home are protected with encryption software.
- Staff have the option to send encrypted emails when necessary.

E-mail

- Pupils use class-based e-mail accounts on the school system.
- Pupils are taught to immediately tell a teacher if they receive offensive e-mail; content of email is closely monitored through class accounts.
- In e-mail communication, pupils are taught not to reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Publishing on the School Website

- Staff or pupil personal contact information will not be published online. The contact details given should be the school office.
- The headteacher will take overall editorial responsibility for any web-based content, and ensure that this is accurate and appropriate.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on any website.

Social networking, gaming sites and instant messenger

- The school will control access to social networking and gaming sites, and educate pupils in their safe use.
- Pupils will be taught never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces, gaming sites and instant messenger outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking and gaming sites.
- Pupils will be made aware of cyber bullying. They will be taught about what this can involve, how it can be avoided and how to deal with it if it occurs.

Managing filtering

- If staff or pupils come across unsuitable on-line materials in school, the site must be reported to the headteacher or deputy head, who will then block the website using 'Study Safe' software.
- A log book will be kept within the school office, where any incidents involving internet misuse, are listed, alongside any action taken. This will be monitored regularly and any findings/patterns used to inform teaching and policy.

Managing webcam use

- Any use of webcams should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before using a webcam.
- Webcam use will always be supervised.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and risk before use in school.
- Staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Children are generally encouraged not to bring their own devices, including mobile phones, into school. If this is unavoidable, they are expected to hand these into the school office as they arrive in the morning and pick them up again at the end of the day.
- Children are not allowed to bring any mobile phones on school trips or to school residential.
- If children bring mobile phones to evening activities such as concerts or School Discos, they are encouraged to leave these with an adult wherever possible.
- The children are made aware that they must not take photographs or videos of members of the school community without their permission and that photographs and videos taken on school premises or at school events must not be uploaded to any websites.

General Data Protection Regulation

- The school is fully compliant with the General Data Protection Regulation (GDPR) and associated Data Protection Bill which replaced the 1998 Data Protection Act. See separate policy.

Digital and video images

- School staff and volunteers will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken

without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the Home School Agreement.

- School staff and volunteers will not use any personally-owned equipment for video, sound or images without prior consent from the headteacher.
- When searching for images, video or sound clips, staff will ensure that they and/or any pupils in their care are not in breach of any copyright law.
- School staff and volunteers will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- Staff ensure that any images taken on school-owned devices are transferred to the school network (storage area/server) and deleted from the memory card/iPad shortly afterwards.
- Images/videos of pupils are deleted shortly after they leave school unless there is a good reason to retain these – e.g. films about residential which may be used to inform younger students.

Staff training

- Staff training in online safety, including issues arising from new technologies, the content of the online safety policy and the use of materials which can be used to support their teaching of the safe use of the internet will be held regularly. This will include regular training (e.g. through INSET) for non-teaching staff.
- Staff should be made aware of their personal responsibilities towards internet use, including social networking sites, both in and out of school. (See appendix)
- When using social networking sites, staff are discouraged from befriending current and past pupils, as well as the parents of pupils who currently attend the school. A number of exceptions will apply to this. This is left to the discretion of the staff involved, depending on their personal circumstances.

Policy Decisions

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Handling online safety incidents

- Complaints of Internet misuse will be dealt with by a senior member of staff and/or Chair of Governing Body.
- Any complaint about staff misuse must be referred to the headteacher and/or Chair of Governing Body.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- If a staff member is a victim of internet misuse - e.g. defamatory comments linked to their work in school on social networking sites - this will be dealt with seriously and reported to the Governing Body; if necessary, help from outside agencies, including the police, will be sought.
- As part of our school curriculum, children will be taught about cyber-bullying; they will learn about what to do if they become victims or if a peer experiences cyber-bullying.
- As part of our school curriculum, children will be taught about what is meant by inappropriate online content and about what to do should they come across this.
- If a pupil becomes a victim of cyber-bullying out of school, this will be dealt with in the same way as any other bullying incident. In addition, parents will be informed, as appropriate, parents/pupils will be asked to retain evidence/screen shots if necessary and positive action will be taken with whole groups/classes of children as required.
- If a pupil comes across inappropriate online content whilst on school premises, the headteacher will be informed and the incident logged. Children will be given the opportunity to talk to an adult, if needed.
- If a pupil comes across inappropriate online content whilst not on school premises, parents and pupils may be offered advice and assistance if required.
- All online safety incidents will be logged in an online safety log book, which will be regularly monitored.

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Children will be asked to sign an age appropriate Acceptable Use Agreement at the beginning of each school year. This could be used to introduce the year's online safety work.
- On occasion, staff and/or governors will interview sample children to ascertain whether they understand how to stay safe on the internet and whether they understand the school's internet safety rules.
- On occasion, children may be surveyed about internet safety in order to inform the scheme and policy.

Staff and the online safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- The online safety policy and the Acceptable Use Agreement will be displayed on the Staff Room notice board.
- The online safety policy will be regularly updated by a team of staff and ratified by governors.

Enlisting parents' and carers' support

- The School online safety Policy will be published on the school website.
- The school will maintain a list of online safety resources for parents/carers, which will be available on the school website.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Occasional training for parents and carers will be offered in safe use of the internet.
- Occasionally, parents/carers and pupils will be surveyed both to inform school about home internet use and to investigate online safety awareness and training needs.

Monitoring and Review

To be reviewed by the Summer Term 2024