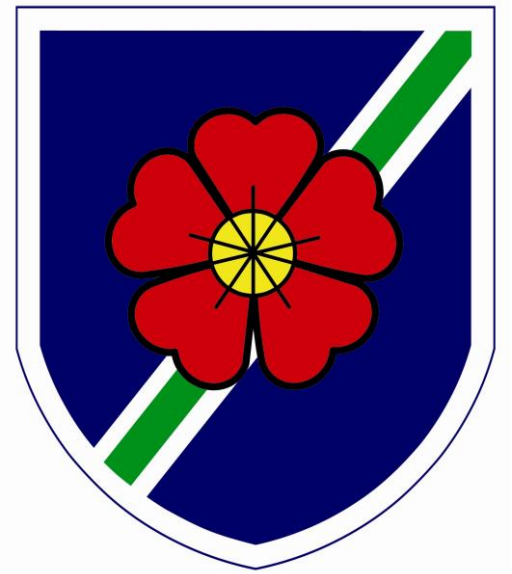
Greenmount Primary School



Policy for

Online Safety

Chronology:
This policy replaces the one agreed by the Governing Body on 22nd May 2022
This policy was discussed and ratified by the Full Governing Body on 20th May 2024.
This policy will be reviewed by the Pupils and Curriculum Committee in the Spring term of 2026.

Introduction

The Governing Body of Greenmount Primary School want all members of our school community to enjoy and benefit from the advantages that technology offers for learning. We do not want the inherent risks associated with access to information, electronic communications and social networking to reduce our use of technology. Instead we want to ensure that our staff, pupils and Governors use the internet in a responsible way so that they do not put themselves or others at risk.

Purpose

The purpose of the online safety policy is to:
- Promote the use of technology within the curriculum.
- Protect children from harm.
- Ensure that the school fulfils its duty of care to pupils.
- Provide clear expectations for staff and pupils on acceptable use of the internet.

At Greenmount we will do this by: -
- Providing a safe internet platform using Surf Protect, which will minimise the chances of pupils encountering unsuitable material.
- Developing a culture of safe practice where everyone is aware of the expected standards of online behaviour.
- Giving staff training a high priority.
- Teaching our children to keep themselves and others safe online and use technology responsibly.
- Ensuring online safety is embedded in the curriculum and actively promoted and a high profile is maintained.
- Running the Smart Squad programme which empowers children to develop their online safety knowledge and share this with their peers.
- Monitor use of the school's computer system by using SENSO and Surf Protect softwares.
- Working in partnership with parents and carers to raise awareness of the potential risks of internet use.
- Ensuring all internet users agree to Acceptable Use Agreement that sets out their rights and responsibilities and incorporates the school's online safety rules before they work on technology.

This policy must be read in conjunction with our "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Our Home-School Agreement states:

The school will:

- teach the children to use modern technologies safely
- only take and publish photos/videos with parental permission

Parents / carers intend to:

- help my child to develop responsible use of modern technologies
- not take photos/videos at school unless permission is given

Roles and Responsibilities

Every member of the school community has a role to play in online safety.

Headteacher
The Headteacher has ultimate responsibility for online safety issues including:
- The development, implementation and review of the school's online safety policy.
- Ensuring that online safety issues are given a high profile within the school community.
- Linking with the Governing Body and parents and carers to promote online safety.
- Ensuring online safety is embedded in the curriculum.
- Ensuring that staff and pupils are aware that any online incident should be reported to them.
- Being the first point of contact and advice for school staff, Governors, pupils and parents.
- Keeping up to date with online safety issues and advise of new trends, incidents or arising problems, including assessing the impact of emerging technology and the school's response to this.
- Managing sanctions against staff and pupils who are in breach of the Acceptable Use Agreement.
- Raising the profile of online safety awareness by ensuring regular staff and governor training.
- Ensuring all staff, pupils and Governors have read and signed the Acceptable Use Agreement.
- Liaising with ICT support to ensure that the anti-virus, filtering and monitoring systems are maintained, audits are carried out and any breaches investigated and records kept.

Governing Body
Members of the Governing Body are subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct.

School Staff
All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils.
Their role is to:
- Adhere to the school's online policy and acceptable use procedures (see "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".)
- Communicate the school's online policy and acceptable use procedures to pupils.
- Engage in online safety training.
- Keep pupils safe and ensure they receive appropriate supervision and support whilst using the internet.
- Plan use of the internet for lessons and researching online materials and resources.
- Report breaches of internet use to the Head Teacher.
- Recognise when pupils are at risk from their internet use or have had negative experiences and take appropriate action. Examples of risk might be inappropriate contact with an adult they have met online; risk from contact with violent extremists; risks from sites advocating suicide, self-harm and anorexia.
- Ensure online safety awareness is embedded in all teaching of PSHE, Computing and other lessons where IT is used so that pupils have the opportunity to discuss issues affecting them in an open and safe environment.
- Be able to access pupil's emails and other internet files generated in school and check these periodically to ensure that expectations of behaviour are being met.

- Be aware of those children with special needs or those who may be more vulnerable to risk from internet use (generally those children with a high level of experience and good computer skills coupled with poor social skills).

Parents and Carers

The school recognises that most children will have internet access at home or on their own mobile devices and might not be as closely supervised as they would be at school.
Children may be put at risk in the following ways:

- By engaging in inappropriate or harmful discussions on social media/chat networks
- By being exposed to inappropriate content e.g. pornography or information advocating violence, suicide or illegal behaviour.
- By having inappropriate contact e.g. through chat rooms, gaming sites, disclosing own personal information or images or cyber bullying.
- By being enticed or persuaded to provide sensitive or private financial information putting themselves or others at risk of unregulated or illegal commercial activity.

The school will work with parents and carers to promote that online safety messages are reinforced at home. We strongly believe that limiting or denying a child access to the internet will not ultimately protect them from the inherent risks. Ultimately we want children to take responsibility for their own choices by understanding the risks and being able to explore online safety issues in the relatively 'safe' environment of school.

The school will:

- Maintain a section on the school website devoted to online safety issues.
- Provide parents/carers with regular online safety updates via the school newsletter.
- Signpost parents/carers to useful resources.
- Alert parents/carers to online safety concerns as they arise (e.g. relating to particular incidents, apps etc).

Each September we ask parents/carers to agree or not agree to visual media of their children being included on the school website and other online platforms that the school uses.

As there is generally not 100% agreement, we ask that parents/carers do not take photographs/videos at school events. School provide to parents/carers or post online photographs/videos in line with the permissions that have been granted.

Further information can be found in "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Pupils

- All pupils are expected to read and agree the Acceptable Use Agreement for Pupils annually having discussed it first with their teachers and parents/carers.
- Pupils are taught to take responsibility for their own behaviour and this includes the material they choose to access on the internet and the content of any online communications.
- Pupils are taught that should they encounter an unsuitable site or be unhappy about any online communications they should alert a member of staff.

Community Use
GOOSE (Greenmount Out of School Experience) is directly run and managed by our governing body. It is an integral part of our school community. Therefore, the policies of the school apply to GOOSE.
Other groups that use our building are not permitted to access the school computer network.

Using the Internet in the Classroom

- Teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- Pupils should not be allowed to aimlessly 'surf' the internet and all use should have a clearly defined educational purpose.
- When using the internet children should receive an appropriate level of supervision for their age and understanding.
- Computers / tablets should not be used at break times unless supervised by an adult or in the area directly outside the staffroom.
- YouTube is a valuable resource but should be used with caution. Children should not search it without close supervision. It is only accessible via staff logins.
- Social Networking Sites, Chat Rooms, Messaging and Gaming Sites are not accessible via the school's network.
- Blogging may only be used if this is monitored by a member of staff.
- If a teacher or pupil unintentionally opens a website with content that is upsetting or inappropriate they should immediately minimise the window. Staff should reassure the pupil they have done nothing wrong and reinforce the online safety message. The incident should be reported to the Head Teacher and the URL and website provided so that the site can be blocked for the future.

Teaching Online Safety

Pupils are taught all elements of online safety included in the PSHE and Computing curricula including but not limited to:
- Keeping personal information private e.g. not to give out personal details to anyone online that may help to identify or locate them or anyone else for example home address, name of school or clubs identified.
- Only using moderated chat rooms that require registration and are specifically for their age group.
- Not uploading personal photos of themselves or others onto sites and to take care regarding what information is posted online as there is no control of who sees images.
- Setting up security and privacy settings on sites.
- Behaving responsibly whilst online and keep communications polite.
- Not responding to any hurtful or distressful messages but to let their parents, carers or teachers know so action can be taken.
- Not arranging to meet anyone whom they have only met online or go offline with anyone they meet in a chat room.
- Identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies In this way they can become responsible, confident, competent and creative users of information and communication technology.

See PSHE Curriculum.

Smart Squad
The school runs a Smart Squad programme. The programme empowers children to keep their friends safe online.
The Smart Squad is a group of children selected from years 4 to 6. The children are set research challenges which they then present to classes across school.

Personal IT Devices (Pupils)

Pupils are allowed to bring a mobile phone with them to school but this must be handed into the class teacher when arriving on site and collected when leaving.
Pupils are not allowed to used phones or other devices during the school day or whilst attending GOOSE or other before/after school activities.

Information relating to staff use of personal IT devices can be found in "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Potential Abuse of the Internet

Intentional access of inappropriate websites by a pupil
If a pupil deliberately accesses inappropriate or banned websites they will be in breach of the Acceptable Use Agreement. The incident should be reported to the Head Teacher who will decide an appropriate course of action.

Inappropriate use of IT by staff or Governors
If a member of staff witnesses misuse of IT by a colleague they should report this immediately to the Headteacher or Chair of Governors. This school's disciplinary procedure will be invoked and followed.

See "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Cyberbullying
Cyberbullying is defined as the use of technology such as email, messaging and social networking sites to deliberately hurt, upset, harass or threaten someone. The internet allows this form of bullying to continue past school hours and invades the victim's home and personal life. It can affect pupils and staff members.
Bullying may take the form of:
- Rude, abusive or threatening messages via email or text
- Posting insulting, derogatory or defamatory statements on blogs or social networking sites
- Setting up web sites that specifically target the victim
- Making or sharing derogatory or embarrassing images or videos of someone via mobile phones or email.

In extreme cases cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

The key points to note are as follows:
1. Any incidents of cyber bullying should be reported to the Headteacher. These will be dealt with in line with our behaviour or anti-bullying policies.
2. Extreme incidents will be reported to the Police.
3. Pupils will be taught
- To only give out mobile phone numbers and email addresses to people they trust
- To only allow close friends whom they trust to have access to their social networking page. Please note that most social networking sites have a minimum age of 13 and as such children and parents will be advised not to have these for primary age children.
- Not to send or post inappropriate images of themselves
- Not to respond to offensive, upsetting or hurtful messages
- To report any problems or worries to their parents and teacher immediately.

Cyber bulling of employees
It is entirely possible that employees at the school may themselves become victims of cyberbullying either by pupils or parents. Further details and advice for employees should be sought from the Head Teacher.

Appendix

Acceptable Use of Technology in School Agreement (Pupils)

Name: _____ Class: _____

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

1. Use the school computers, tablets, Internet and all our technological equipment sensibly and carefully.

2. Only use the username and password I have been given to access the computer network.

3. Ask permission before entering any website, unless my teacher has already approved that site.

4. Not use YouTube without an adult's permission.

5. Not tell people about myself online. (I will not tell them my name, anything about where I live or where I go to school or upload any photos.)

6. Always be polite and kind and use appropriate language when communicating online.

7. Tell a member of staff immediately if I see anything I am unhappy with or I receive messages I do not like.

8. Not respond to any nasty message that makes me feel upset or uncomfortable.

9. Only e-mail people or open e-mails from people I know, or my teacher has approved.

10. Not look at or delete other people's files without their permission.

I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.

Signed: _____ Date: _____-