Greenmount
Primary School

Greenmount Primary School

E-SAFETY POLICY

October 2022

Together, we nurture the future

1 Document Information

Title:	**e-Safety Policy**
Status:	**Final**
Current Version:	1.2
Author(s):	Kiitan Alabie, eSafety Co-ordinator
Approving Committee:	Full Governing Body
Approved by:	Catherine Powell, Chair of Governors
Approval Date:	
Review Frequency:	Annually
Next Review	Autumn Term 2023

Version History

Version	Date	Description
1.0	Autumn 2018	Initial version
1.1	July 2019	Converted to standard format
1.2	Autumn 2022	Minor changes, re-numbering of content and updates in line with latest government legislation.

2 Contents

3 Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information

- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Access to sites that promote extremism
- The potential for excessive use, which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

4 Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school computing systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are of the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which make take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where know, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

5 Policy and Leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with Computing. It also outlines the core responsibilities of all users of computing devices in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of Computing.

5.1 Governing Body

Greenmount Primary School has a named safeguarding governor who works with senior leaders to ensure that the governing body regularly:

- Review and monitor this e-safety policy.
- Consider any issues relating to school filtering
- Discuss any e-safety issues that have arisen and how they should be dealt with

In addition, the safeguarding governor has a responsibility to

- Attend regular meetings with the E-Safety Co-ordinator with an agenda based on:
  - monitor e-safety incident logs
  - monitor filtering change control logs
  - monitor logs of any occasions where the school has used its powers of search and deletion of electronic devices
- report outcomes of monitoring to the FGB

The governors will support the school in encouraging parents and the wider community to become engaged in e-safety activities.

5.2 eSafety Co-ordinator

The eSafety Co-ordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The eSafety Co-ordinator:

- works with and reports regularly to governors, SLT and the School Council on e-safety development
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school eSafety policy and guidance.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident (including recording incidents on CPOMS)
- provides training and advice for staff
- liaises with the school IT Technician
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets with the safeguarding governor to discuss current issues and review incident logs
- attends relevant meetings and committees of Governing Body
- receives appropriate training and support to fulfil the role effectively
- has responsibility for passing on requests for blocking/unblocking internet sites to the IT Technician

5.3 IT Technician

The IT Technician is responsible for ensuring that:

- The school's IT infrastructure is secure and is not open to misuse or malicious attack
- Users may only access the school's network through a properly enforced password protection policy
- Short-comings in the infrastructure are reported to the eSafety Co-ordinator and SLT so that appropriate action may be taken.

5.4 Headteacher

The head teacher is responsible for ensuring the overall safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is designated to the eSafety Co-ordinator.

The head teacher will:

- ensure the school uses an approved filtering internet service, which complies with current statutory requirements.
- ensure that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- receive regular monitoring reports from the IT Technician
- take overall responsibility for data and data security

The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. See flow chart on dealing with e-safety incidents (Section 9) and relevant Local Authority HR/LADO and disciplinary procedures.

5.5 Classroom based staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood, signed and adhere to the school's Acceptable Use Policy
- they understand and promote the school's e-safety and related safeguarding policies, including PREVENT guidance
- they report any suspected misuse or problem to the eSafety Co-ordinator and record the incident on CPOMS.
- digital communications with students (email/Google Classroom) are no a professional level and only carried out using official school systems and never through personal mechanisms e.g. email, text, mobile phone
- e-safety issues are embedded in the curriculum and other school activities
- they model safe, responsible and professional behaviours in their own use of technology

- they maintain an awareness of current online safety issues and guidance through research and personal development

5.6 Pupils

The pupils are responsible for ensuring that they:

- understand the importance of reporting abuse, misuse or access to inappropriate materials
- know and understand school policy on the use of mobile phones, digital cameras and hand held devices
- know what action to take if they or someone they know feels worried or vulnerable when using online technology
- know and understand school policy on the taking/use of images and on cyber-bullying
- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school
- take responsibility for learning about the benefits and risks of using the internet and other technologies safely, both in school and at home
- help the school in the creation/review of e-safety policies

5.7 Parents/Carers

Parents and carers are expected to:

- support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement, which includes the pupils' use of the internet and the school's use of photographic and video images
- read, understand and promote the school Pupil Acceptable Use Agreement with their children
- access the school website in accordance with the relevant school Acceptable Use Agreement

6 Acceptable Use Policies

All members of the school community are responsible for using the school computer systems in accordance with the appropriate Acceptable Use Policy (AUP), which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix A.

Acceptable use policies are revisited and re-signed annually at the start of each school year and amended accordingly in the light of new developments. Copies are sent home for further discussion with parents/carers.

Parents/Carers sign once when their child enters the school. The Parents' policy also includes permission for use of their child's image (still or moving) by the school; permission for their child to use the school's computing resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each academic year.

7 Self Evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school (in particular the annual Section 175 audit tool). The views and opinions of all stakeholders (pupils, parents, staff) are taken into account as a part of this process.

8 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on computing equipment provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files

- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

8.1 Pupil Sanctions

	Refer to class teacher	Refer to e-safety	Refer to head teacher	Refer to Police	Refer to e-safety	Inform parents / carers	Removal of network /	Warning	Further sanction e.g.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√		√	√	√	√	√
Unauthorised use of non-educational sites during lessons	√				√		√		
Unauthorised use of mobile phone / digital camera / other handheld device	√		√			√			
Unauthorised use of social networking / instant messaging / personal email	√				√				
Unauthorised downloading or uploading of files	√				√				
Allowing others to access school network by sharing username and passwords	√	√	√		√		√		
Attempting to access the school network, using another pupil's account	√	√	√		√		√		
Attempting to access or accessing the school network, using the account of a member of staff	√	√	√				√		
Corrupting or destroying the data of other users	√	√	√			√	√	√	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√			√		√	

Continued infringements of the above, following previous warnings or sanctions	√	√	√	√		√	√	√	√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√			√		√	
Using proxy sites or other means to subvert the school's filtering system	√	√	√		√		√	√	
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√	√		√	√			
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√	√	√		√	√	√	√	

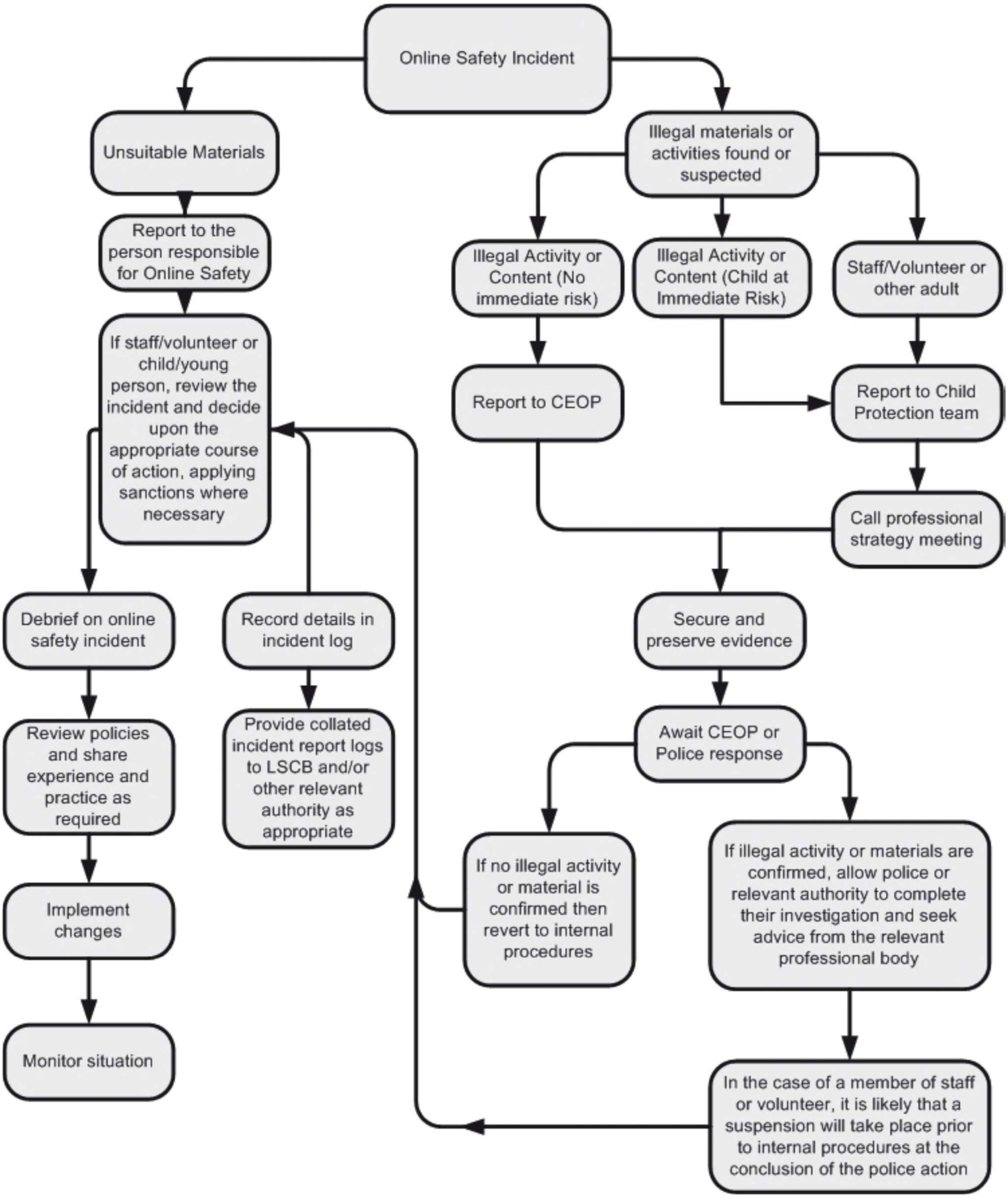
8.2 Staff Sanctions

	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√	√			√	√		
Unauthorised downloading or uploading of files	√	√			√	√		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	√	√				√		
Careless use of personal data eg holding or transferring data in an insecure manner	√	√				√		
Deliberate actions to breach data protection or network security rules	√	√			√	√	√	

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√	√			√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√			√	√	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	√	√	√			√		
Actions which could compromise the staff member's professional standing	√	√				√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√				√		
Using proxy sites or other means to subvert the school's filtering system	√	√			√	√	√	
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√			√	√		
Deliberately accessing or trying to access offensive or pornographic material	√	√	√		√	√	√	
Breaching copyright or licensing regulations	√	√				√		
Continued infringements of the above, following previous warnings or sanctions	√	√	√			√	√	√

9 Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of computing devices, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

10 Audit/Monitoring/Reporting/Review

The e-Safety Co-ordinator will ensure that full records are kept of incidents involving the searching of mobile phones and electronic devices and the deletion of data/files.

These records will be reviewed by the head teacher/and a governor on a termly basis.

11 Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
  - personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
  - staff are permitted to use these devices in school but not whilst working with children
- pupils are not currently permitted to use their personal hand held devices in school, and must hand them to a member of staff, to be stored securely, if they have them on site.

12 Email

Access to email is provided for all users in school via Google Gmail, which is accessible via a web browser on all computer devices (PCs, laptops, chromebooks).

These official school email services may be regarded as safe and secure and are monitored.

- Users need to be aware that email communications may be monitored.
- A structured education programme is delivered to pupils, which helps them to be aware of the dangers of and good practices associated with the use of email.
- Users must immediately report (to their class teacher/eSafety Co-ordinator) in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

13 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use , sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images, that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

14 Use of web-based publication tools

Our school uses a public facing website (www.greenmount.iow.sch.uk) for sharing information with the community beyond our school. This includes, from time to time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff (never pupils).
- Only pupils' first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and comply with the following good practice guidance on the use of such images:
    - Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - Written permission from parents and carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

15 Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf. Teachers translate these standards appropriately for all matters relating to eSafety.

Any digital communication between staff and pupils or parents/carers (email, chat, VLE, etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat/social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

16 Filtering

16.1 Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from RM, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at a local level.

16.2 Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the eSafety Co-ordinator and IT Technician (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard RM school filtering service must:

- Be logged in change control logs
- Be authorised by a second responsible person prior to changes being made (this will normally happen anyway, as part of the process and will be the class teacher who originally made the request for the change).

All users have a responsibility to report immediately to class teachers/eSafety Co-ordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

16.3 Education/training/awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- Signing the AUP (a part of their induction process)
- Briefing in staff meetings, training days, etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety updates on our website/newsletter, etc.

16.4 Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

16.5 Audit/reporting

Logs of filtering change controls and of filtering incidents are made available to

- E-safety Co-ordinator
- Safeguarding Governor

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

17 E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing, PSHE and other lessons and should be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school
- We use the resources on CEOP's Think U Know site (http://www.thinkuknow.co.uk/teachers/resources) as a basis for our e-safety education (Hector's World at KS1 and Cyber Café at KS2). We also have access to resources via our subscription to SCARF (https://www.coramlifeeducation.org.uk/scarf) and the National Online Safety Hub (https://nationalonlinesafety.com/lesson-plans).
- Learning opportunities for e-safety are built into the Computing scheme of work where appropriate and are used by teachers to inform teaching plans.
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of Computing devices both within and outside school.
- In lessons where the internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

17.1 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address)
    - Cross checking references (can they find the same information on other sites)
    - Checking the pedigree of the compilers/owners of the website
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require.

17.2 The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school. Members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices), could be helpful in their learning.

17.3 Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff via our subscription to the National Online Safety Hub.
- It is expected that some staff with identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction.
- The e-Safety Co-ordinator will receive regular updates through attendance at local authority or other information/training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- The e-Safety Co-ordinator will provide advice, guidance and training to individuals as required on an on-going basis.

17.4 Governor training

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee or group involved in Computing, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the local authority, National Governors Association or other bodies and via the school's subscription to the National Online Safety Hub.
- Participation in school training/information sessions for staff or parents

The safeguarding governor works closely with the e-Safety Co-ordinator and reports back to the full governing body.

17.5 Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site

- Parents evenings
- Reference to the parents materials on the Think U Know website and the National Online Safety Hub

17.6 Wider school community understanding

Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents/carers. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community users who access school computer systems/website/VLE as part of the Extended School provision will be expected to sign a Staff, Governors, Volunteers and Visitors AUP (See Appendix A) before being provided with access to school systems.

18 Links to other policies and guidance

This policy has strong links to other school policies as follows:

- Anti-bullying policy
- PSHE & RSE policy
- Safeguarding and Child Protection policies
- Behaviour policy

The following government guidance was referenced in the formation of this policy:

- Keeping children safe in education (2022)
- Teaching online safety in schools (2019)
- Education For A Connected World Framework(2020)

Appendix A – Acceptable use policies (AUPs)

Staff, Governors, Volunteers and Visitors

GREENMOUNT PRIMARY SCHOOL

Acceptable Use of ICT

Agreement for Staff, Governors, Volunteers and Visitors

Acceptable use of the school's ICT facilities and the internet: Agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including, but not limited to, material of a violent, criminal or pornographic nature (or create, share , link to or send such material) • Use them in any way which would harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside of school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the Designated Safeguarding Lead (DSL) and IT Technician know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed:	**Date:**

Parent/Carer

GREENMOUNT PRIMARY SCHOOL

Acceptable Use of the Internet

Policy Agreements and Permissions Form

Acceptable Use of the Internet: Agreement for Parents and Carers

Name of Parent/Carer:

Name of Child:

Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels:

- Parentapp (for school announcements and information via push notifications, email and text)
- Our virtual learning platform (Google Classroom)

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues if they are not raised in an appropriate way.
- Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident.
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers.

Signed:	**Date:**

Acceptable Use of the School's ICT Facilities and Internet in school: Agreement for Pupils and Parents/Carers

Name of Pupil:

When I use the school's ICT facilities in school (like computers and equipment) and access the Internet in school, I will:

- Ask a teacher before signing on
- Observe school rules
- Only use websites approved by the school

- Not access social networking sites or chat rooms (unless my teacher said I could as part of a lesson)
- Check with my teacher before opening any attachments in emails, or clicking any links in emails
- Be polite and respectful online
- Keep my password safe and not use anybody else's password

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I am aware there will be consequences given by school if I do not follow the rules when using devices online (both in school and outside of school).

Signed (pupil):	**Date:**

Parent/Carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (Parent/Carer):	**Date:**

Permissions to use digitial images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by name.

As the parent/carer of the above pupil, I agree to the school taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events, where permitted, which include images of children, I will abide by these guidelines in my use of these images.

Signed (Parent/Carer):	**Date:**

Permission to publish my child’s work (including on the Internet)	
It is our school’s policy, from time to time, to publish work of pupils by way of celebration. This includes on the internet; via the school website. As the parent/carer of the above child, I give my permission for this activity.	
Signed (Parent/Carer):	**Date:**

Appendix B – Guidance for reviewing internet sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs, etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case, please refer to the flowchart for responding to online safety incidents and report immediately to the police.

Please follow all steps in this procedure:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken of site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of ‘grooming’ behaviour
    - The sending of obscene materials to a child

    Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

    It is important that all the above steps are taken as they will provide an evidence trail for the group (possibly the police) and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix C – Criteria for website filtering

ORIGIN – What is the website's origin?

- The organisation providing the site is clearly indicated.
- These is information about the site's authors (about us, our objectives, etc.)
- There is a contact for further information and questions concerning the site's information and content.

DESIGN – Is the website well designed?

- Is it appealing to its intended audience (colours, graphics, layout)?
- Is it easy to navigate through the site – links are clearly marked, etc?
- Does it have working links?
- Does it have inappropriate adverts?

CONTENT – is the website's content meaningful in terms of its educational value?

- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- The site promotes equal and just representations of racial, gender and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful/unsuitable for the pupils .
- Is the website current?

ACCESSIBILITY – Is the website accessible?

- Loads quickly?
- Does the site require registration or passwords to access it?
- Does the site require usage fees to be paid?