Greenholm Primary
Greenholm Road
Great Barr
Birmingham
B44 8HS
0121 464 6321

GREENHOLM PRIMARY

ESAFETY POLICY

Overarching statement
At Greenholm we are a school that is welcoming, safe and creates an environment which values and supports everyone learning. We work hard to create an ethos that promotes inclusive practice for all, by providing a consistent and fair approach, which is supportive of the continual emotional development of all and by demonstrating mutual respect, openness and honesty.

Vision Statement
At Greenholm we believe that educating children to safety use ICT will prepare them to be safe and secure when using all forms of ICT both now and in their future education and employment. We want all members of the school community to know how to deal with situations as they encounter them.

Rationale
As a school we believe that educating children to safety use ICT, rather than limit their use, will prepare them to participate in a rapidly changing world in which work and other activities are increasingly dependent on developing technologies. At school and home our pupils need to use ICT to find, explore, analyse, exchange and present information, as well as communicate with others. They need to be taught how to do this in a safe way to enable them to use ICT responsibly. Students need to be taught and encouraged to report incidents with the confidence they will not be blamed, educating and encouraging them to deal with issues in a sensible and appropriate manner. In order for this to happen the adults around them also need to understand the possible risks, how to minimise these and what to do in the event of inappropriate use or accidental discovery of inappropriate content.

> *'Schools have a major responsibility to educate their pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies'.*
> (Becta E-safety guidance)

Aims
For all members of the school community to have a clear understanding of their role in ensuring their own and others safety when using ICT and that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
To have clear procedures for members of the community to follow should an incident occur.
For all members of the school community including children teachers and parents to be given relevant and up to date e-safety training that includes emerging technologies as well as those already embedded in the school.
For appropriate filters to be in place within school to minimise the risk of inappropriate material being accessed.
To provide an environment where children can ask advice on e-safety issues and know how to report.
To ensure that instances of breaches in safety and security and abuse of ICT are logged and reported to the appropriate person and dealt with according to the appropriate policy.

Related Policies:

Child Protection	Acceptable User Policy	Curriculum Policy
Safeguarding	Mobile Phone Policy	School Media Policy
Health and safety	Anti-Bullying Policy	Staff Induction Policy
Home/ School Agreement	Data Protection Policy	Visitor Policy

ICT Committee

Safeguarding

The main areas of risk for our school community can be summarised as follows:

Content

exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
lifestyle websites, for example pro-anorexia/self-harm/suicide sites
hate sites
content validation: how to check authenticity and accuracy of online content

Contact

grooming
cyber-bullying in all forms
identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Cyberbullying

Cyber bullying is taken very seriously and the curriculum provides opportunities for pupils to discuss the internet and some of the precautions they should take. Pupils know that if cyber bullying is taking place they should notify their teacher or a senior member of staff immediately. Incidents that occur outside of school but impact on school life should be reported to the Head teacher where they will be investigated. This is also taught alongside traditional bullying as per the anti bullying policy

Managing E-mail

All use of e-mail within the school is regulated and monitored. Staff, pupils and students must use the approved school email account based upon the school system. A member of the leadership team or the ICT technician should be informed immediately if they receive anything deemed offensive or could potentially cause damage to the school's network. Any use of non-school e-mails for correspondence could be in breach of the DATA protection act as the e-mail systems used may not be as secure as the school's systems.

Internet Access

All staff, students and KS2 pupils will read and agree the 'Acceptable Use Agreement' before using any school ICT resource and will reminded of the agreement wherever appropriate. Within foundation stage and Key Stage 1 access to the Internet will be led by adult demonstration, directly supervise activities and approved online materials. The school has the right to monitor internet use via Policy Central.

School Website

The school website plays a key role in communicating key information about school with parents. Only photos of pupils are uploaded where consent has been given by parents/guardians. Only forenames will be published and surnames will NOT be used. Home information and e-mail identities will not be included, only the point of contact to the school i.e. school phone number, school address and enquiry e-mail address. Uploading of information is restricted to our website authorisers - the technical support manager. The school website complies with the statutory DfE guidelines for publications.

Twitter and Social Media

The school's account is designed to celebrate successes of the school
All photos tweeted must be within school guidelines and policies in place to protect pupils
Photos and full names (including surnames) must not be posted together as it is deemed personal identifiable information
Tweets must not include anything listed in the inappropriate behaviour section above
All use must be in user with other key school policies such as the social media policy – see this for further protocols and procedures

Passwords and Access to School Systems
In accordance with the School's 'Acceptable User Policy':
All staff are made aware of the importance of having a secure password
All staff are to ensure their workstation is locked when not being used
All staff must ensure they do not give out passwords to allow access to school systems
Personal data must be saved on shared network drives that students do not have access to

Staff Development
Each year staff are reminded of the e-safety training they should be teaching their children, this could be in line with Anti-Bullying week. This is appropriate to the year group, age and experience of the children they are currently teaching. Material to support staff in keeping themselves safe are also circulated as new risks become apparent.

Curriculum:
E-Safety will be promoted by e-safety posters and messages prominently displayed in classrooms and other learning areas, particularly the ICT suite. Reminders of e-safety rules and the acceptable use policy are displayed whenever technology is used. Discussion of e-safety issues and risks, and strategies for dealing them, are carried out at appropriate points throughout the curriculum. E-safety assemblies or theme days are held throughout the year, specifically Safer Internet Day each February or Anti-Bullying Week each November. E-safety is discretely taught as part of using technologies across the curriculum, covering the following objectives

Reception
To know that you should only use programs an adult has directed you to.
To know what to do if they see something that makes them feel uncomfortable.

Year 1
To know not to share information about themselves with people they talk to online
To know not to download files (click yes) without permission
To know what to do if they see something that makes them feel uncomfortable.

Year 2
To know the SMART rules for online safety
To know what to do if they see something that makes them feel uncomfortable.
To know the different ways in which they access the internet (i.e. phones, games consoles etc.)

As children become more proficient in using ICT independently, and are able to use ICT in school with less supervision and direction the following objectives become vital and must be taught and revisited each year.

Throughout KS2 Pupils are taught about the safety and 'netiquette' of using e-mail and social media both in school and at home i.e. they are taught:
not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
that an e-mail is a form of publishing where the message should be clear, short and concise;
that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
that they should think carefully before sending any attachments;
embedding adverts is not allowed;
that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
not to respond to malicious or threatening messages;
not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
that forwarding 'chain' e-mail letters is not permitted.

Year 3
To know what to do if they see something that makes them feel uncomfortable.

Year 4
To know about copyright laws and how this can affect what they do online (i.e. using other's pictures, information and downloading music and films)
To know what to do if they see something that makes them feel uncomfortable.
To know who to talk to if they have concerns about their safety online (i.e. through cyberbullying or if they think they have given out information they shouldn't)

Year 5
To understand bias and reliability
To know what to do if they see something that makes them feel uncomfortable.
To know who to talk to if they have concerns about their safety online (i.e. through cyberbullying or if they think they have given out information they shouldn't)

Year 6
To understand the importance of protecting information online
To have an awareness of social media and how to keep safe
To know what to do if they see something that makes them feel uncomfortable.
To know who to talk to if they have concerns about their safety online (i.e. through cyberbullying or if they think they have given out information they shouldn't)

Expected conduct
In this school, all users are expected to:
To read, understand and help promote the school's e-safety policies and guidance
To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
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
to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
To maintain an awareness of current e-safety issues and guidance e.g. through CPD
To model safe, responsible and professional behaviours in their own use of technology
To ensure that any digital communications with pupils are on a professional level and only through school based systems i.e. school email, never through personal mechanisms, e.g. personal email, text, mobile phones etc.
be responsible for keeping themselves safe both in and outside school in line with the social media policy and mobile phone policy.
Teachers
To embed e-safety issues in all aspects of the curriculum and other school activities
To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Students/Pupils
should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
be aware of things they can do to keep themselves safe (SMART) rules

Parents/Carers
should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
should discuss the SMART rules with their children, showing them how to use the internet safely on all the devices their children come into contact with

need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so both within and outside of school
Access support materials such as the CEOP website and the Think you know websites
Support the school by reinforcing the e-safety messages the children are given by taking part in activities sent home especially as part of the Safer Internet and Anti Bullying days.

Specific role of the **Technical Support Team** to support the e-safety within the school community
To ensure all firewalls, filters and anti virus protection is up to date and effective.
To report any failures of the filters to the appropriate filter management company or ISP.
To log any incidents in the e-safety incidents book in pen, signed and dated.
To keep abreast of relevant e-safety legislation
To review and update e-safety policies and procedures regularly inline with current guidelines

Specific role of the **ICT Curriculum co-ordinator** to support the e-safety within the school community
embedding e-safety in staff training, continuing professional development and across the curriculum and learning activities
To ensure involvement in the key e-safety days, providing information for staff and parents and delivering assemblies
To review and update e-safety policies and procedures regularly in line current guidelines
To ensure that planning includes notes for staff to remind children of the key safety points to consider at the beginning of lessons when using ICT
To ensure E-safety procedures are displayed in both classrooms and the ICT suite and that these are updated as necessary
To ensure planning includes information on copyright infringement so that this can be taught and that children are encouraged to reference any material they have used from other sources.
To keep abreast of relevant e-safety legislation
To undertake relevant e-safety training
To ensure parents are aware of their role in e-safety and are sufficiently informed.

E-safety incident Procedures.

In the case of suspected cyber bullying or inappropriate conduct between pupils within or outside of school, all involved parties with be dealt with in line with the school's behaviour and anti bullying policies and hierarchy of consequences. See additional notes on cyber bullying.

In the case of inappropriate material being viewed - the monitor should be turned off and a senior member of staff should be sent for. The link should be noted down and given to the ICT technical support manager so that this can be fed to the filter management company to prevent further access. The incident should be logged in the E-Safety incident book which is kept in the head teachers' office.

Any case of parent, pupil or ex pupil making inappropriate contact or any other breech of security or professional relationship using e-media should be logged in the E-safety incident book which is kept in the head teachers' office. However it is staff's responsibility to ensure all efforts are be made to minimise the risk of this happening through the use of security settings on any social networking and the sole use of staff email accounts for contact with the school community. In line with the social media policy. All correspondence should be filed within staff email system.

Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
The Police will be notified if one of our staff or pupils receives online communication that the school considers particularly disturbing or suspects breaks the law.
Where pupils deliberately access inappropriate material or use e-mail inappropriately action will be taken by the headteacher or a member of the leadership team and parents or guardians notified in line with the behavior policy.

Monitoring
This policy and the acceptable user policies should be regularly reviewed by the ICT strategy team to take into account the ever increasing technologies available to our school community.