Green Oak

ACADEMY

E-Safety Policy

Updated: September 2018

Next review: September 2020

Ratified by the Chair of Governors

Name: Mawlana Maseehullah Patel

Signature:

Green Oak Academy
E-Safety Policy

The E-Safety Policy will be reviewed every 2 years, but may be reviewed and updated more frequently if necessary, in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys/questionnaires of:
  - students
  - parents/carers
  - staff

What is e-safety?

The School's e-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

e-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- e-Safety concerns safeguarding children and young people in the digital world.
- e-Safety emphasises learning to understand and use new technologies in a positive way.
- e-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- e-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable pupils to use on-line systems safely.

The School need to protect itself from legal challenge and ensure that staff work within the boundaries of professional behaviour. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use email, text or instant messaging (IM) to ‘groom’ children.

Green Oak Academy makes it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is “unauthorised” and ensure an Acceptable Use Policy is in place. e-Safety training is an essential element of staff induction. However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that e-Safety is an ever growing and changing area of interest and concern. The school’s e-Safety policy must reflect this by keeping abreast of the vast changes taking place around us.

The school’s e-Safety Policy must operate in conjunction with other school policies including Behaviour, Child Protection and Anti-Bullying. e-Safety must be built into the curriculum.

Our Vision

Green Oak Academy embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Green Oak Academy aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by staff and pupils while on the school premises.

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The designated senior person for child protection is Mrs Amenah Dabhelia.

All members of the school community have certain core responsibilities within and outside the school environment.
They should:

- Accept responsibility for their use of technology.
- Use technology responsibly.
- Model best practice when using technology.
- Report any incidents to senior leadership.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Physical Environment / Security
The school endeavours to provide a safe environment for the whole community. We review both physical and network security regularly as well as monitor who has access to the system.

- Anti-virus software is installed on all computers and is updated regularly.
- The school makes sure that all network computers are used as ensure compliance with the Acceptable Use Policies.(**Appendix 1 and Appendix 2)**
- Due to the type of data kept on the Admin network it is necessary to keep this network physically separate from the Curriculum network and comply with a more rigorous security setup.
- All pupils are issued with their own username and password for network access and understand that this must not be shared.

Mobile / emerging technologies
Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understands that the Acceptable Use Policies apply to this equipment at all times.

- Staff understand that they should use their own mobile phones sensibly and in line with schools e-safety policy.
- Pupils are not allowed to use their mobile phones in school. They have to hand them in, to the office.
- Pictures/videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

Digital Media

We respect the privacy of the school family. If we have direct instructions not to publish or share a specific pupil’s image or video, then we will refrain from doing so in the public space.

- Photographs and/or videos of pupils in school must only be taken using the school’s equipment. Personal cameras and or phones should not be used.

Guidelines / Good Practice

It is normally possible to block/ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site.

Many social network providers also enable users to pre-moderate any comments left on their profile before they are visible by others. This can help a user prevent unwanted or hurtful comments appearing on their profile for all to see. The user can also set their profile to 'Private,' so that only those authorised by the user are able to access and see their profile.

If social networking sites do receive reports about cyber bulling, they should be able to investigate and may remove content that is illegal or breaks their terms and conditions in other ways. By reading the terms and conditions you will be able to see information on what is inappropriate and unacceptable behaviour, as well as providing prominent safety information so that you know how to use the service safely and responsibly.

It is advised to report any incidents of unpleasant comments posted on these sites and also take steps to have them removed. The procedure for different sites is provided below.

FACEBOOK

There are different ways to stop bullying on Facebook, depending on the type of bullying. You can remove tags or block people who are sending you nasty messages. You can also report abusive posts or groups so Facebook can take them down. Reports are anonymous so the person doing the bullying won't know who reported it.

The way to report abuse changes depending on what you are reporting.
https://www.facebook.com/help/420576171311103/

It's a really good idea to set your profile to 'friends only' so that you can't be on the end of bullying from people you don't know.

You can find the Terms of Service by following this link:
http://www.facebook.com/terms.php?ref=pf

YouTube

YouTube can be a great online video community – but it's important to follow their safety guidelines. Bullying on YouTube could happen through videos themselves or through the comments that people post on videos. YouTube has a very strict policy on what's allowed in videos, comments and general behaviour. If the bullying is in a video you can report it by clicking the 'flag' button underneath the video. If you want to report cyber bullying or abuse through comments or private messages then you can use

YouTube’s reporting tool link:
http://www.youtube.com/yt/policyandsafety/reporting.html

Instagram

Instagram can be a great way to share photos with your friends, but some people try to use it for cyber bullying instead. Sometimes people might write nasty comments on an image or upload embarrassing photos of someone. Instagram is automatically set to public so that anyone can see your images - even if you don’t know them. It’s much easier to stop bullying if your profile is private. When your profile is private, anyone who wants to follow you and see your photos has to send you a request - which you can ‘approve’ or ‘deny’. This way you can control who sees your photos and can make sure only your friends can talk to you on Instagram. You should also report anyone who is being abusive to you by using the link below:
http://help.instagram.com/165828726894770/

Snapchat

Snapchat can be a really fun way to share images. It’s different from other photo sharing apps because when you send an image, it will only last between 1 and 10 seconds before being deleted. If someone is bullying you on Snapchat, blocking them will stop them from sending abusive messages. You can also report bullying to Snapchat - they may be able to help stop it.
https://support.snapchat.com/en-GB/article/report-abuse-in-app

Twitter

The School does not provide twitter usage policy therefore it does not take any responsible for publishing tweets.

Staff will not use Twitter’s private messaging facility to communicate with current school pupils under any circumstances.

Appendix 1

GREEN OAK ACADEMY INTERNET ACCEPTABLE USE POLICY

Green Oak Academy believes that the benefits to students from access to the internet far exceed any disadvantages of access. These benefits include access to information resource and opportunities for collaboration.

Students and their parents should be aware that some internet sites may contain material that is illegal, defamatory, inaccurate or offensive to some people. The school believes that ultimately, parents and guardians of students are responsible for setting and conveying the standards that their child should follow.

Green Oak Academy is able to exercise the normal requirement for supervising students accessing the internet, however the school does not have control of the information on the internet, nor can it guarantee to provide electronic barrier to prevent students accessing the full range of information available.

By agreeing to the Internet Acceptable use policy, the student agrees to abide by the restriction outlined in this policy. The student and her parents or guardians should discuss these rights and responsibilities.

The student is held responsible for her actions and activity when using internet. Unacceptable uses of internet will result in the suspension or revoking of internet access privileges. Examples of such unacceptable use are:

- Using the internet for any illegal activity, including violation of copyright.
- Damaging or disrupting equipment or software.
- Interfering with data of another user or invading the privacy rights of other users.
- Wastefully using finite resources.
- Posting personal communication without the original author’s consent or anonymous messages.
- Viewing, downloading, storing, or printing files or messages that are obscene, or that use language that offends or trends to degrade others.
- Knowingly introducing a computer virus to any of the school computer systems.
- Violating the content guidelines as outlined below.

CONTENT GUIDELINES: Students who are allowed to produce materials for publication on the internet are constrained by the following guidelines.

Students work published on the internet must not contain any personal identifying information such as home telephone numbers and addresses.

ACCEPTABLE USE KIT

When using the Internet I agree to:

Protect my privacy rights and those of other students by not giving out personal details including full names, telephones numbers, addresses and images.

Use the internet in line with my school’s student code of conduct and use appropriate language when talking to and working online with others and never participate in hate mail.

Use the internet at school for educational purposes and use the equipment properly.

Use social networking sites for educational purposes and only as directed by teachers.

Not deliberately entering or remaining in any site that has obscene language or offensive content (e.g racist material or violent images)

Abide by copyright procedures when using content on websites (ask permission to use images, text, audio, video and cite references where necessary)

Think about how I use the content posted on the Internet and not simply copy and paste information from websites.

Not interfere with the network security, the data of another user or attempt to log into the network with the user name or password of another student.

Not reveal my password to anyone except the system administrator or classroom teachers.

Not to bring or download any unauthorised programs including games, to the school or run them on the school computers.

Talk to my teacher or another adult if:

- I need help online
- I feel that my welfare of other students at the school is being threatened by online activities
- I come across sites which are not suitable for our school
- Someone writes something I don't like or makes me and my friends feel uncomfortable or ask me to provide information that I know is private.

I have read the internet-acceptable use kit carefully and understand the significance of the conditions and agree to abide by these conditions. I understand that any breach of these conditions will result in the internet access privileges being suspended or revoked

Student Name:..
Year:................................

Student Signature: ....
Date:..............................

Parent Signature: ....
Date:..............................

Appendix 2

ACCEPTABLE USE AGREEMENT (Staff/Volunteer)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that staff are protected from potential risk in their use of ICT in their everyday work. Green Oak Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users. This policy applies to any device in school. It applies across the whole network and includes WiFi.

Green Oak Academy carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Green Oak Academy can read the information and remove inappropriate content or prevent access to the material.
For my professional and personal safety:

- I understand that Green Oak Academy will monitor my use of the ICT systems,
- I understand that the rules set out in this agreement also apply to Green Oak Academy ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that Green Oak Academy ICT systems are primarily intended for educational.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the School ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive

or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities

Green Oak Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where personal data transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened. When using the internet in my professional capacity or for school sanctioned personal use.

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

ACCEPTABLE USE AGREEMENT (Staff/Volunteer)
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:……………………………………………………

Signed:……………………………………………………………………

Date:…………………………………………………………………………