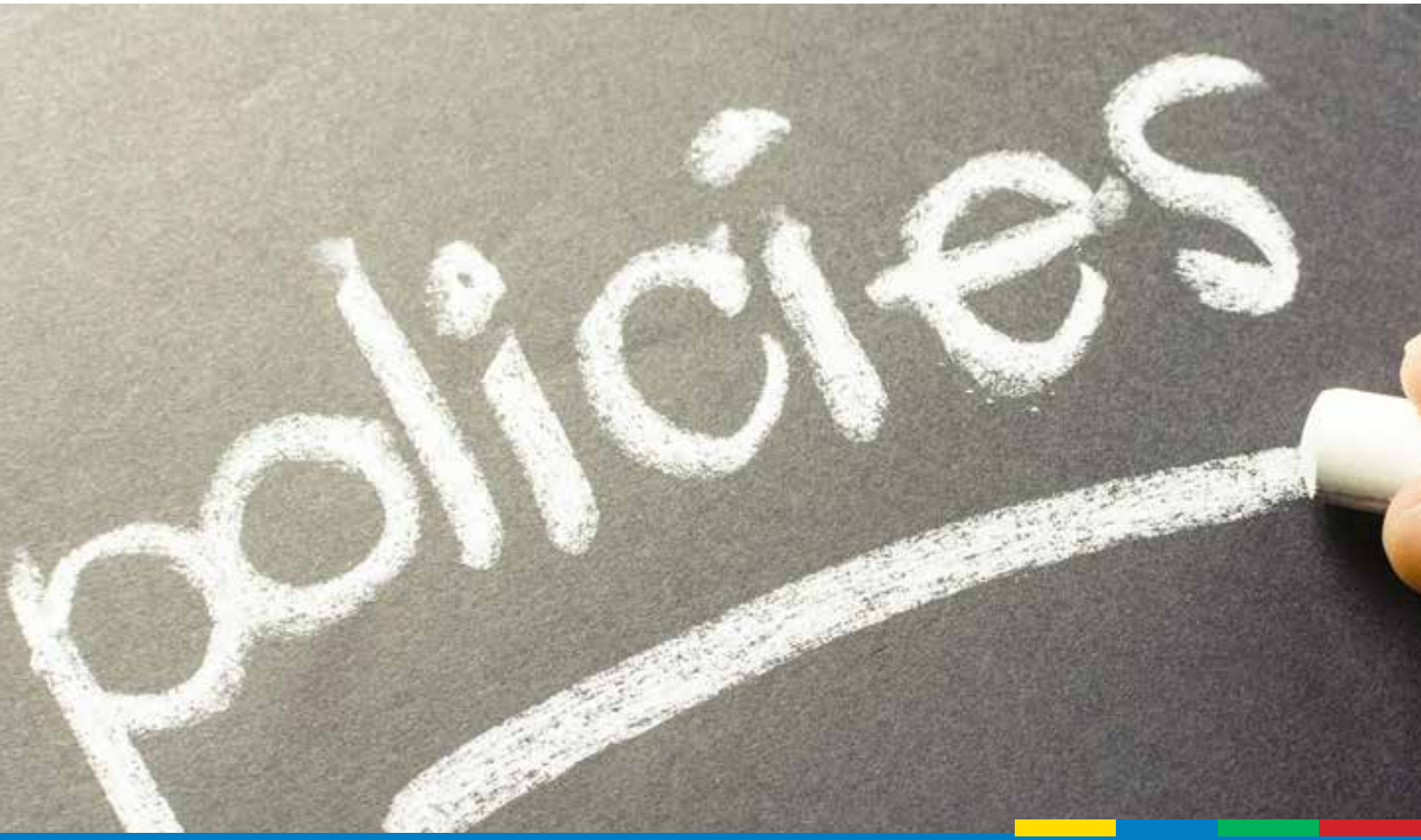
GREAT BARR ACADEMY
A SPECIALIST SCIENCE COLLEGE
NURTURING POTENTIAL
CREATING OPPORTUNITY



E-SAFETY POLICY

2015-**2016**

E-SAFETY POLICY

GREAT BARR ACADEMY
A SPECIALIST SCIENCE COLLEGE
NURTURING POTENTIAL
CREATING OPPORTUNITY

1. Introduction:

1.1

Great Barr School (the School) recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

1.2

However, the rapid pace of development of the internet and communication technologies can present schools and employers with new and often unforeseen challenges and potential risks. The School aims to implement appropriate safeguards within the School, supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. As part of our duty to safeguard and promote the welfare of our students, we will do all that we can to keep our students e-safe and ensure that our staff promote a culture of e-safety.

1.3

This policy should be read in conjunction with the Acceptable Usage Policies for students and for staff and volunteers and alongside other relevant policies:

i. Child Protection Policy
ii. Anti-Bullying Policy
iii. Mobile Phone Policy
iv. Dignity at Work Policy
v. Disciplinary Procedure
vi. Social Media Policy
vii. Acceptable Usage of IT Equipment Policy
viii. Data Protection Policy

2. Monitoring:

2.1

The Safeguarding Group, chaired by the Headteacher, will take responsibility for monitoring the implementation of the policy and for carrying out periodic reviews of its effectiveness.

2.2

It is recognised that this policy must be reviewed and revised regularly in response to the ever-changing ICT environment within and outside the School.

3. Scope of the Policy:

3.1

The policy applies to:

i. All users (staff, volunteers and students) who have access to the School's IT systems or equipment, both on the premises and remotely.

ii. All use of the Internet and all forms of electronic communication such as email, mobile phones, social media sites (eg. Facebook and Twitter), blogs, forums, discussion groups, online chat facilities (Skype, MSN etc), SMS and MMS, smartphone apps etc.

iii. The School's wired and wireless IT network and all computing and communications technology owned and/or managed by the School.

4. Monitoring Internet Access:

4.1

To minimise risk to pupils, the School will continue to adopt a centralised Internet filtering system designed to prevent access to sites with undesirable or inappropriate content.

4.2

We recognise that the Internet changes daily and that no technological solution can be 100% effective in guaranteeing online safety. The filtering system is therefore monitored regularly by GBIT to find evidence of inappropriate searches or access to websites with undesirable content in order to add new sites to the filtering system and identify those who might be misusing the system.

4.3

Staff supervising children using IT equipment will be vigilant in monitoring activity.

4.4

Where a student is found to be deliberately misusing the Internet, staff will:

i. immediately withdraw the student's access to the Internet
ii. Refer the matter appropriately using BFL
iii. Notify the GBIT Manager who will maintain a log of incidents and pass this to the Safeguarding Group for routine review.

The student's system access may be withdrawn altogether for a period and their parents may be informed in order that they can be made aware of the potential need to monitor home usage more rigorously.

4.5
In the event of a child being unintentionally exposed to undesirable materials:

i. The child should notify a teacher immediately
ii. The teacher should inform the GBIT Manager.
iii. Where appropriate, House staff will be notified and will determine whether and how parents should be notified.
iv. The incident will be recorded by the GBIT Manager such that the School may reliably report the frequency and nature of incidents to the Safeguarding Group and can review whether further control measures are required to prevent a reoccurrence of the incident.
v. Parents or Governors may be notified at the discretion of senior staff according to the degree of seriousness of the incident

4.6
All users are warned that the School reserves the right to access any data, files, emails etc. stored in the user area or on any devices (including staff or student laptops, Memory sticks, CD ROMs, DVDs or student's mobile phones) at any time.

4.7
The School also reserves the right to monitor all incoming and outgoing communications using the School's computer systems.

5. Promoting Safe Usage:

5.1
E-safety will be addressed as a discrete topic in the following areas of the curriculum:

i. Year 7 ICT lessons. One of the first units of work studied by all Year 7 groups covers e-Safety. This 8-lesson unit aims to teach children how to protect themselves from the human and technological dangers posed by the Internet.
ii. Year 7 Library Induction. Given the importance of the internet as an information resource, the Librarian includes e-safety in the Induction programme for new students.

We will also seek opportunities to cover e-safety in the new PSHE curriculum.

5.2
The School will make use of opportunities outside the curriculum to promote messages about safe and responsible usage of the Internet, Social Media and other communications technologies, through assemblies, for example.

5.3
Before embarking on a lesson involving Internet usage, teachers will remind children:

i. To tell them immediately if they accidentally come across an inappropriate site.
ii. Of the consequences of deliberately accessing/ searching for sites not connected with the task in hand.

5.4
The School has a comprehensive Social Media Policy which aims to provide clear guidance to staff, regulate their conduct online and ensure that appropriate professional boundaries are in place at all times between staff and students in relation to all forms of communication technologies.

5.5
All staff and volunteers registered on the School's system are provided with an Acceptable Usage of ICT Equipment Policy (see attached). Failure to adhere to the policy will result in reasonable management action being taken which could include formal action under the Disciplinary Procedure.

5.6
All student planners include an Acceptable Usage of ICT Equipment Policy. Failure to follow the policy will result in consequences under the BFL system.

5.7

The School subscribes to the 'Sharp' system through which students can report any issues of concern online directly to the Deputy Head Teacher (Pastoral). This provides a safe mechanism for students to report e-safety and other concerns.

CONT.....

5.8
The School believes that parents have a role in promoting e-safety and monitoring their children's Internet usage. When logging onto the Parent Zone, all users are faced with a pop-up box encouraging them to be mindful of e-safety issues and directing them to a comprehensive and reputable source of advice and guidance online – the NSPCC website which has a whole section on e-safety.

6. Use of Images:

6.1
The School will give all parents and carers the opportunity annually to notify the School that they do not consent to images of their child being used in publications which may be viewed outside the School, eg. the website, newspapers, the Prospectus or other marketing literature. The form sent to parents will notify them that non-return of the form will provide consent for their child's image to be used.

6.2
Staff taking photographs of children for any purpose which might involve publication outside the School will obtain the list from Reception of children for whom the School does not have parental consent to use their images and will ensure that the children listed are not included in photographs. Additionally, they will tell the children the purpose for which the images are being taken, how they will be used and where they will be published before taking the photographs and give the pupils the opportunity to opt-out if they wish.

6.3
Where pictures of pupils are posted on websites, only the pupil's first name will be used to prevent them from being identifiable except where explicit permission has been obtained from the child's parent.

6.4
Images of staff will only be published with their explicit verbal consent.

6.5
In accordance with the Social Media Policy, staff should never post pictures of pupils on their personal social media sites in any circumstances.

This policy was agreed and adopted by the Governing Body on 7 October 2014.

Acceptable Usage of ICT Equipment Policy (Staff)

All staff and volunteers registered on the School's system are provided with an Acceptable Usage of ICT Equipment Policy (see attached). Failure to adhere to the policy will result in reasonable management action being taken which could include formal action under the Disciplinary Procedure.

Professional Conduct:

- You must keep your username and password safe and secure. You must not share it, nor must you try to use another person's username and password. You should not write down or store a password where it is possible that someone may steal it.

- You must ensure that you understand the School's Social Media Policy and act in accordance with it at all times.

- You must only use the School's IT systems/ equipment for very limited personal or recreational use and such activity should primarily be carried out outside working time. If you are found to be using significant amounts of working time using ICT equipment for personal use, you will be subject to disciplinary action.

- You must never use the School's IT equipment to upload, download or access or attempt 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), inappropriate, may cause harm or distress to others or which might compromise your professionalism. Any material which you would not be entirely happy for the Headteacher to see is likely to meet this definition.

- If you accidentally access any illegal, inappropriate or harmful material or become aware that another member of the School community has accessed such material, you must immediately report the matter to the GBIT Manager, the HR Manager or the Deputy Headteacher (Pastoral). A record will be kept of such disclosures for future reference even where no further action is necessary.

- You must not access, copy, remove or otherwise alter any other user's files, without their express permission.

E-SAFETY POLICY

GREAT BARR ACADEMY
A SPECIALIST SCIENCE COLLEGE
NURTURING POTENTIAL
CREATING OPPORTUNITY

- Your electronic communications with others must be professional in tone and manner; you should act in accordance with the School's Dignity at Work Policy at all times.

Digital Images & Video:

- When you take and/or publish images of others, you must do so only after explaining the purpose for which the photographs are being taken, how they will be used and where they will be published and after being given their explicit verbal permission.

- You must never publish images of children whose parents have denied the School permission to use such images; an up to date list of these pupils can be obtained from Reception.

- If you use your own camera or mobile phone to record these images, you should delete the images as soon as you have transferred them to your School computer.

- Where you have supervised a trip or any other school related activity and have taken some photographs of students as a personal memento, you may retain these on your personal IT equipment at home but, in accordance with the School's Social Media Policy, you must never publish the photographs on personal social media sites or anywhere else.

- If you publish images of students on the school website or VLE, for example, you should not publish the child's surname or any other person information except their first name unless explicit permission has been gained from the child's parents/carer.

Responsible use of equipment:

- As a member of staff, you have a duty to safeguard and promote the welfare of young people. Teaching staff and others working directly with students should make use of all opportunities to encourage safe and responsible use of ICT equipment and to ensure that children are alert to and understand the dangers. You should also carefully monitor usage amongst the children you are supervising and, where necessary, take prompt and appropriate steps to remove children from risk of harm and alert an appropriate member of the senior or Pastoral staff.

- When you use your personal mobile devices (laptops / mobile phones / USB devices etc) in school, you must follow the rules set out in this agreement in the same way as if you were using school equipment. You must ensure that any such devices are protected by up to date anti-virus software, are free from viruses and present no foreseeable risk to the School's systems.

- You must not open any hyperlinks in emails or any attachments to emails unless you know and trust the person/ organisation who sent the email or if you have any other concerns about the email.

- You must never try to disable or bypass the School's filtering/security systems.

- You must not make large downloads or uploads which might take up significant internet capacity and prevent other users from being able to carry out their work unless you have sought prior permission from the GBIT Manager.

- You must not install or attempt to install or store programmes of any type on any school device or try to alter computer settings unless authorised by GBIT.

- You must keep private and confidential any staff or student data to which you have access except where it is appropriate and lawful to disclose such information to an appropriate authority or external agency.

- You must only use or process staff or student data for the purposes for which it was provided.

- You must report any damage or faults involving equipment or software as quickly as possible, however this may have occurred.

- Where work is protected by copyright, including music and videos, copies can be downloaded for educational use in school but must not be downloaded for personal use.

- When you use your personal mobile devices (laptops / mobile phones / USB devices etc) in school, you must follow the rules set out in this agreement in the same way as if you were using school equipment. You must ensure that any such devices are protected by up to date anti-virus software, are free from viruses and present no foreseeable risk to the School's systems.
- You must not open any hyperlinks in emails or any attachments to emails unless you know and trust the person/ organisation who sent the email or if you have any other concerns about the email.

- You must never try to disable or bypass the School's filtering/security systems.

- You must not make large downloads or uploads which might take up significant internet capacity and prevent other users from being able to carry out their work unless you have sought prior permission from the GBIT Manager.

- You must not install or attempt to install or store programmes of any type on any school device or try to alter computer settings unless authorised by GBIT.

- You must keep private and confidential any staff or student data to which you have access except where it is appropriate and lawful to disclose such information to an appropriate authority or external agency.

- You must only use or process staff or student data for the purposes for which it was provided.

- You must report any damage or faults involving equipment or software as quickly as possible, however this may have occurred.

- Where work is protected by copyright, including music and videos, copies can be downloaded for educational use in school but must not be downloaded for personal use.

You should be aware that:

- This Acceptable Usage Policy applies not only to your work and use of School ICT equipment in school, but also applies to your use of such systems and equipment off the premises, to your use of personal equipment on the premises and to situations related to your employment by the School.

- Failure to comply with this Acceptable Usage Policy could lead to disciplinary action and/or, in the event of illegal activities, the involvement of the police.

- All School devices and systems are monitored. The School has the right to access emails sent by you and to you through the School's systems and to inspect any activity undertaken on or content held on any ICT equipment issued to you by the School for professional use.

Acceptable Usage of ICT Equipment Policy (Students)

The School will try to ensure that you have excellent access to digital technologies to enhance your learning and, in return, expects you to be a responsible user. All students must follow this code of conduct at all times.

Staying Safe Online:

- You must keep your username and password safe and secure. You must not share it, nor must you try to use another person's username and password. It is good practice not to write down or store a password where it is possible that someone may steal it.

- You must be aware of "stranger danger" when you are communicating online.

- You must not disclose personal information about yourself or others when online. This could include names, addresses, email addresses, telephone numbers, age, gender, where you go to school etc.

- If someone is asking you for your personal details online, I must talk to your parents or a teacher about it straight away.

- You must NEVER send or post pictures of yourself online or through your mobile which you would not be happy for your parents or teachers to see. Once the image is sent, you have lost control of what can be done with it; it may be used to harm you. If we become aware of such behaviour, we will do everything we can to keep you safe. We will ALWAYS inform your parents and we may need to involve the police.

- If you arrange to meet people offline that you have communicated with online, you must only do so in a

public place and you must take an adult with you.

- You must immediately report any unpleasant or inappropriate material or messages or anything that makes you feel uncomfortable when you see it online.

- If you are the victim of cyber-bullying, try to keep copies of the postings/ messages / texts and raise it immediately with a parent or the House staff. You also use the Sharp system to report such behaviour.

Responsible use of equipment:

- IT systems and devices are provided for educational use. You must only use them in accordance with your teacher's instructions; you must not use them for recreational use.

- You must respect others' work and property and must not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.

- You must be polite and responsible when you communicate with others.

- You must never try to contact School staff online except through the School email system.

- You must not take or distribute or print pictures or video of anyone without their permission.

- You must never try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.

- You must immediately report any damage or faults involving equipment or software, however this may have happened.

- You must not open any hyperlinks in emails or any attachments to emails unless you know and trust the person/ organisation who sent the email or if you have any other concerns about the email.

- You must not install or attempt to install or store programmes of any type on any school device or try to alter computer settings.

- You must never try to disable or bypass the School's filtering and security systems.

- Where work is protected by copyright, including music and videos, copies can be downloaded for use as part of your school work but must not be downloaded for personal use.

- You must avoid wasting paper, only printing what you have to print when you are sure no more changes are needed.

You should be aware that all school devices and systems are monitored. The School has the right to access your emails at any time. The School also has a legal right to confiscate your mobile phone or any other personal device, to examine the content held on it, and to store it securely.