Green Park Village
PRIMARY ACADEMY

Enabling Excellence for Exceptional Futures

Policy name:	e-Safety Policy
Policy group:	Safeguarding
Policy status:	Recommended
Linked REAch2 policy(ies)	REAch2 Safeguarding and Child Protection Policy
Policy owner:	Gemma Jackson- Head Teacher
Written/ Adopted/ Reviewed on:	Adopted: May 2020
Review date due:	Summer 2022

REAch2
ACADEMY TRUST
EXCEPTIONAL OPPORTUNITIES FOR LEARNING

Document Control

This policy should be read in conjunction with:

- Acceptable Internet Usage agreement (Staff)
- Acceptable Internet "Safe and Respectful Use" Agreement Policy (Children)
- Behaviour Policy
- Anti-Bullying Policy
- Anti-racism Policy
- Health and Safety policy (includes positive handling)
- Whistleblowing an Public Interest Disclosure
- Personal, Social, Health and Moral Education Policy
- Staffing Policy
- Procedures to handle allegations against other children
- Staff behaviour policy (code of conduct)

The Designated Safeguarding Lead is: Gemma Jackson
The Deputy or the person to contact in his/her absence is: Lucy Newman
The Local Safeguarding Children Board (LSCB) is Berkshire West Safeguarding Children Partnership (BWSCP).
The e-safety lead in school is: Gemma Jackson

POLICY

At Green Park Village Primary Academy we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

E-Safety is concerned with protecting young people in the digital world and ensuring they feel safe when accessing new technology. The School will comply with the Ofsted expectations set out in the Ofsted handbook, which outline the following expectations that need to be met:

- All teaching and non-teaching staff should be aware and able to recognise e-safety issues;
- Clear emphasis on training to all staff with one member of staff to receive accredited training;
- Clear reporting processes;
- Policies and procedures integrated with other relevant policies;
- Progressive e-safety curriculum;
- Good risk assessment;
- Pupils need to feel safe at school and must "have an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites".
- Pupils should "work hard with the school to prevent all forms of bullying, including online bullying and prejudice-based bullying".
- Staff and pupils should "deal effectively with the very rare instances of bullying behaviour and/or use of derogatory or aggressive language".
- In addition, pupils should "have an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites".

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Use of the internet

The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images;
- Cyber bullying;
- Access to, or loss of, personal information;
- Access to unsuitable online videos or games;
- Loss of personal images;
- Inappropriate communication with others;
- Illegal downloading of files;
- Plagiarism and copyright infringement;
- Sharing the personal information of others without the individual's consent or knowledge.

E-safety control measures

<u>Educating pupils:</u>

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the school;
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online;
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism;
- Clear guidance on the rules of internet use will be presented in all classrooms;

- Pupils are instructed to report any suspicious use of the internet and digital devices, e.g. Report of Abuse CEOP.

Educating staff:

- All staff will undergo e-safety training on a termly basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety;
- All staff will undergo regular audits by the e-safety lead in order to identify areas of training need;
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices;
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand the E-safety Policy.

Internet access:

- Internet access will be authorised once parents/carers and pupils have returned the signed consent form as part of the Acceptable Internet "Safe and Respectful Use" Agreement Policy;
- A record will be kept by the Head Teacher of all pupils who have been granted internet access.
- All users in key stage 2 and above will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details;
- Pupils' passwords will be changed on a regular basis, and their activity is continuously monitored by the e-safety lead;
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity;
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites;
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Head Teacher;
- All school systems will be protected by up-to-date virus software;
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers;
- The master users' passwords will be available to the Head Teacher for regular monitoring of activity.

Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts;
- Use of personal email to send and receive personal data or information is prohibited;
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email;
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending;
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Social networking:

- Access to social networking sites will be filtered as appropriate;
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Head Teacher;
- Pupils are regularly educated on the implications of posting personal data online, outside of the school;
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole;
- Staff are not permitted to communicate with pupils over social networking sites.

Published content on the school website and images:

- The Head Teacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate;
- All contact details on the school website will be the phone, email and address of the school. No personal details of staff or pupils will be published;
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received;
- Pupils are not permitted to take or publish photos of others without permission from the individual;

- Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment, eg personal mobile phones, tablets.

Mobile devices:

- The Head Teacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use;
- Mobile devices are not permitted to be used in the classroom by pupils or members of staff;
- The sending of inappropriate messages or images from mobile devices is prohibited;
- Mobile devices must not be used to take images of pupils or staff;
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

Cyber bullying:

- For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online;
- The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur;
- The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online;
- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils;
- The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying Policy;
- The Head Teacher will decide whether it is appropriate to notify the police of the action taken against a pupil.

Reporting misuse

Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use;
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Head Teacher, using a complaints form;
- Any pupil who does not adhere to the rules outlined in our Acceptable Internet "Safe and Respectful Use" Agreement Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use;
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the head teacher and will be issued once the pupil is on the school premises;
- Complaints of a child protection nature shall be dealt with in accordance with our Safeguarding and Child Protection Policy.

Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the head teacher, using a complaints form;
- The Head Teacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.

ROLES AND RESPONSIBILITES

The governing body will ensure that:

- All staff who work with children undertake regular safeguarding training;
- The local governing body reviews its policies/procedures annually;
- A designated governor is appointed with a specific brief for safeguarding and child protection and will liaise with the Head Teacher and DSL. The role is strategic rather than operational – they will not be involved in concerns about individual pupils/students;
- The designated governor will liaise with the Head Teacher and the DSL to produce an annual report for governors;
- Regular meetings are held with the e-safety lead to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs.

- **The Head Teacher will:**
- Be responsible for the implementation of the policy and ensuring that the outcomes are monitored;
- Be responsible for ensuring that the e-safety lead and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff;
- Ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school;
- Review and amend this policy with the e-safety lead, taking into account new legislation and government guidance, and previously reported incidents to improve procedures;
- Communicate with parents regularly and updating them on current e-safety issues and control measures;
- Establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff;
- Report annually to the governors on the working of the policy.

- **The School E-Safety Lead will:**
- Be responsible for ensuring the day-to-day e-safety in our school and managing any issues;
- Provide all relevant training and advice for members of staff on e-safety;
- Regularly monitor the provision of e-safety in the school and return this to the head teacher;
- Report Cyber bullying incidents in accordance with the school's Anti-Bullying Policy.
- Ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

- **The Designated Safeguarding Lead (DSL)**

The DSL is a senior member of staff, who undertakes lead responsibility for safeguarding and child protection within the school. The DSL will:

- Be the first point of contact for parents, pupils, teaching and non-teaching staff and external agencies in all matters of child protection;
- Ensure that all cases of suspected or actual problems associated with safeguarding children are investigated and dealt with;
- Be aware of the latest national and local guidance and requirements and keeping the Head Teacher and staff informed as appropriate;
- Consult with the Head Teacher on an appropriate training programme;
- Ensure that appropriate training for staff is organised according to the agreed Ensure that adequate reporting and recording systems are in place;
- Liaise with the Governing Body's Nominated Governor for safeguarding children.

All pupils will:

- Ensure they understand and adhere to the Acceptable Internet "Safe and Respectful Use" Agreement Policy, which they must sign and return to the Head Teacher.

Staff will:

- Ensure they understand and adhere to the Acceptable Use Policy, which they must sign and return to the head teacher;
- Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
- Be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the school and to deal with incidents of such as a priority;
- Ensure they are up-to-date with current e-safety issues, and this E-safety Policy.

Parents and Carers are:

- Responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

Personal data must be managed securely and in accordance with the statutory requirements of the General Data Protection Regulation 2018.

Any professional communication that takes place through technology must be transparent and open to scrutiny, take place within explicit boundaries and must not be shared with young children.