



Enabling Excellence for Exceptional Futures

Policy name:	Online Safety and Acceptable Use 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 Reviewed: January 2021
Review date due:	Summer 2022



Online Safety Policy

“Safeguarding is everybody’s business”

This policy should be read in conjunction with:

- Acceptable Internet Usage agreement (Staff)
- Acceptable Internet “Safe and Respectful Use” Agreement Policy (Learner) *Appendix 1*
- Acceptable Internet Use and Acceptable Use of Technology Agreement – Staff *Appendix 3*
- Remote Learning- using online video communication Agreement for parent *Appendix 2*
- Learner Attitudes (Behaviour) Policy
- Anti-Bullying Policy
- Health and Safety Policy – Trust and School
- Whistleblowing Policy
- Personal, Social, Health and Moral Education (PSHE) Policy
- Remote Learning Policy

The Designated Safeguarding Lead is: Gemma Jackson

The Deputy or the person to contact in her absence is: Lucy Newman

The Local Safeguarding Children Board (LSCB) is: Berkshire West Safeguarding Children Partnership (BWSCP).

The internet 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.

Internet safety is concerned with protecting young people in the digital world and ensuring they feel safe when accessing new technology. Here are the expectations we believe need to be met:

- All teaching and non-teaching staff should be aware and able to recognise internet 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 internet 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.

Internet safety control measures

Educating pupils:

- An internet 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 internet 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 internet safety training on a termly basis to ensure they are aware of current internet safety issues and any changes to the provision of internet safety;
- All staff will undergo regular audits by the internet 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 internet safety training as part of their induction programme, ensuring they fully understand the Internet 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 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 internet safety lead, in conjunction with the REAch Central IT Team;
- 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 REAch Central IT Team 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:

- All staff are provided with work mobile devices, such as an iPad, for use in school;
- The Head Teacher may authorise the use of personal mobile devices by a pupil where it is seen to be for safety or precautionary use;
- Personal 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 CPOMS incident reporting;
- 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;
- 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 RESPONSIBILITIES

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 internet safety lead to discuss the effectiveness of the internet 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 internet 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 internet safety officer, whose role is to carry out the monitoring of internet safety in the school;
- Review and amend this policy with the internet 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 internet 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 Internet safety Lead will:**
- Be responsible for ensuring the day-to-day internet safety in our school and managing any issues;
- Provide all relevant training and advice for members of staff on internet safety;
- Regularly monitor the provision of internet 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 internet 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 local 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 (Appendix 1), 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 internet 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 internet safety issues, and this Internet safety Policy.

Parents and Carers are:

- Responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.
- Ensure they understand and adhere to the Acceptable Internet “Safe and Respectful Use” Agreement Policy (Appendix 1), which they or their child must sign and return to the Head Teacher.
- Ensure they understand and adhere to the “Remote Learning- using online video communication Agreement for parent” (Appendix 1), which they must sign and return to the Head Teacher.

Extreme circumstances- Agreements may be signed via Forms during periods of school closure.

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.



Acceptable Internet “Safe and Respectful Use” Agreement Policy- Learners

1. I will not use school ICT equipment until I have signed and agreed to the Acceptable Internet “Safe and Respectful Use” Agreement.
2. I will use the computers and other ICT equipment only for my learning during lesson times and only on permitted sites and apps; including during golden and privilege times.
3. I will only go online or use the Internet at school when a staff member gives permission.
4. I will only search for things online that I know are acceptable at our school. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.
5. If I have my own class user account, I will log on only with that class name and I will keep my password private.
6. I will use my class or school email address when emailing in school and I will keep my password private.
7. I am representing my school anytime I use the Internet, e-mail, mobile phones or any ICT equipment. I will only use it for positive purposes, not to be mean to others, or in any way harm anyone else, or the school itself. This includes using the internet outside of school time.
8. If I see or hear of any other pupils not following the *Acceptable Internet “Safe and Respectful Use” Agreement*, I will report it to an adult straight away.
9. Only with permission from school will I bring in any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives. I will take responsibility for this and the school is not liable for any loss or damages.
10. To ensure my compliance with copyright laws, I will download or copy any files such as music, videos, games or programs only with the permission of a staff member or the owner of the original material.
11. I will not give out any of my personal information online, both in and out of school. This includes:
 - my full name;
 - my address;
 - my e-mail address;
 - my phone numbers;
 - photos of me and/or people close to me.
12. I will respect all school ICT equipment and will treat all devices with care. This includes:
 - following the rules given when using each device;
 - reporting any breakages/damage to a staff member;
 - being mature and responsible when handling the equipment.
13. I will only delete or open my own files.
14. I will only open e-mail attachments from people known to me or people whom my teachers have approved.
15. I will make sure ICT communication with other pupils and adults is polite and responsible.
16. I will not send pupils or adults any content which is unpleasant. If I find something like this, I will report it to a staff member.
17. I will not meet someone unless it is part of a school project and/or a responsible adult is present with me.
18. I am responsible for my behaviour while using ICT.
19. I will not upload images, sound, video or text content that could upset pupils, staff and others.
20. I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my e-safety.
21. If I see something online that makes me feel uncomfortable, I will inform my class teacher.

Name: _____ Signed: _____

Class: _____ Date: _____



Remote Learning- using online video communication Agreement for parents

Through supporting my child in using video communication, I agree to ensure that:

- a parent is present (same room/ ear shot) during online / live communication; a parent is present (beside/near to the child) for one to one sessions with their child and a teacher;
- my child wears suitable clothing (clothes/ covered up/ top and a bottom) – this includes others in my household;
- where possible, my child will be situated in a suitable ‘public’ living area within the home with an appropriate background-‘private’ living areas within the home, such as bedrooms, should ideally be avoided during video communication;
- my child uses appropriate language – this includes others in my household;
- my child maintains the standard of behaviour expected in school, following the instructions/ guidance/ request of the teacher online;
- my child uses the necessary equipment and computer programs as intended; video material is not recorded, stored, or distributed without permission;
- I have a stable connection to avoid disruption to lessons (where possible);
- my child (and passing family members) remain aware that they are, or could be, visible on screen.

Child’s name:		Date:	
Parent’s name:		Parent’s signature:	



Acceptable Internet Use and Acceptable Use of Technology Agreement – Staff

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the Head Teacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. Using technology in school

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the Head Teacher.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other pupils, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given by the Head Teacher for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the Head Teacher.
- I will only store data on removable media or other technological devices that has been encrypted or pseudonymised and where permission has been given by the Head Teacher or REAch2 IT.
- I will provide removable media to the Head Teacher for safe disposal once I am finished with it.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.

- I will ensure that mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.
- I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the Head Teacher before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the Head Teacher.
- I will not use personal and school-owned mobile devices to communicate with pupils and the Head Teacher will approve/ be aware of communication with parents, when outside of the school's main office@ contact email.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the Head Teacher or REAch2 IT Team to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Head Teacher before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Working at home

-
- I will adhere to the principles of the GDPR when taking work home.
- Where possible, school assigned device will be used for all home working/ working at home.

- I will ensure I obtain permission from the Head Teacher before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the Head Teacher before it is used for lone-working.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.

5. Training

- I will ensure I participate in any online safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Head Teacher or REAch2 IT Team undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the Head Teacher.
- I understand that my use of the internet will be monitored by the REAch2 IT Team and recognise the consequences if I breach the terms of this agreement.
- I understand that the Head Teacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Staff member

Signed:

Date:

Print name:

Head Teacher

Signed:

Date:

Print name:
