


Green Park School E-Safety Policy for Early Years

Policy written by:	Angie Esson
Role:	Computing Curriculum Leader
Committee approving Policy	Standards Committee
Date approved by Committee:	20 May 2024
Date for renewal:	Every 3 Years, Summer 2027 Reviewed & updated FEBRUARY 2024
Signed by Chair of Committee	 Linda Guest, Chair of Governors

Our Mission

Green Park aims to provide access to high quality education and learning experiences, both in school and in the community and seeks to maximise each pupil's achievement as part of his or her lifelong learning. It is the school's aim to be a centre of Educational Excellence in the heart of the community.

Context

The internet is an accessible tool to all pupils.

All educational settings have a duty to ensure that children are protected from potential harm both within and beyond the learning environment.

Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate the risks. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

Aims

- To offer valuable guidance and resources to Green Park School and practitioners to ensure that they can provide a safe and secure online environment for all children in their care.
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies in the school setting.

Scope of Policy

This policy applies to all staff, children, parents/carers, committees, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above mentioned groups, such as mobile phones, personal devices and all electronic devices with imaging and sharing capabilities. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop or mobile phones, personal devices and all electronic devices with imaging and sharing capabilities.

At Green Park, we provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. Children learn in an environment where security measures are balanced appropriately with the need to learn effectively. Our school community understand the importance of an eSafety Policy.

Staff Responsibilities

Practitioners (including volunteers)

- Our eSafety Champion and Online Safety Lead is Angela Esson.
- The role of the eSafety Champion in our school ensuring that the eSafety Policy and associated documents are up to date and reviewed regularly;
- Ensuring that the policy is implemented and that compliance is actively monitored;
- Ensuring that all staff are aware of reporting procedures and requirements should an eSafety incident occur;
- Ensuring that the eSafety incident log is appropriately maintained and reviewed regularly;
- Keeping up to date with eSafety issues and guidance through liaison with the School IT Team;
- Ensuring eSafety updates, training and advice is available for staff, parents/carers and governors;
- Liaison with Senior Designated Person(s) to ensure a coordinated approach across relevant safeguarding issues.

All staff have a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

Broadband and Age Appropriate Monitoring & Filtering

Broadband provision is essential to the running of our school setting, not only allowing for communication with parents and carers but also providing access to a wealth of

resources and support. Many settings now use internet enabled devices, including iPad educational apps and games, to enhance the learning experience of children or as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available regardless of the size of the setting.

Monitoring and Filtering levels are managed and monitored on behalf of the setting by Wolverhampton Schools technical support team.

Email Use - Staff

The setting provides all staff with access to a professional email account to use for all work related business. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

All emails should be professional in tone and checked carefully before sending, just as an official letter would be.

Email is covered by the Data Protection Act (1988) and the Freedom of information Act (2000) so safe practise should be followed in respect of record keeping and security. All staff is aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy. All users must report immediately any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Use of Social Networking Sites (advertising or parental contact)

At Green Park School, Social networking sites (e.g. Facebook and Twitter) are used as an advertising tool for Green Park School. Due to the public nature of social networking and the inability to keep content truly private, best practice guidance states that:

- Identifiable images of children should not be used on social networking sites.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- Ensure that privacy settings are set to maximum and checked regularly.
- For safeguarding purposes, photographs or videos of any child including Children and Young People in Care Children must not be shared on social networking sites.
- Staff will not 'like' Green Park School post to protect their social media identity.

Please note: Green Park does not endorse the use of photographs or video featuring children and young people on sites such as Facebook and Twitter, due to issues with obtaining parental consent and the inability to ensure that the privacy of those young people can be safeguarded on social networking sites.

Mobile phones, personal devices and all electronic devices with imaging and sharing capabilities

Many existing mobile phones, personal devices and all electronic devices with imaging and sharing capabilities, such as portable media players, PDAs, gaming devices, and smart phones are familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Green Park chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile phones, personal devices and all electronic devices with imaging and sharing capabilities

Green Park allows staff to bring in personal mobile phones, personal devices and all electronic devices with imaging and sharing capabilities for their own use. Under no circumstances does Green Park allow a member of staff use this device whilst working or in areas where children are allowed during the school day – even if the room is empty and the children are on the playground. All personal devices must be switched off and locked away during the school day. They can be used in the staff room or areas that are not designated for pupil use. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Green Park is not responsible for the loss, damage or theft of any personal mobile phones, personal devices and all electronic devices with imaging and sharing capabilities. Parents, visitors, volunteers, contractors, Governors and individuals engaged by the school are not permitted to use their phones in the presence of pupils anywhere within the school building.

Should staff need to receive e.g. emergency information about their child from their child's school or information about acutely ill dependents or family members, the school work number must be given to the appropriate parties. Once they contact the school, the admin team will contact the staff member appropriately.

Decisions regarding special arrangements will be made on a case-by-case basis by the headteacher. If special arrangements are not deemed necessary, school staff can use the school office number **01902 556429** as the point of emergency contact.

Smart Watches

Fitbits and most fitness trackers are harmless – they track steps taken, heart rate, and remind adults to walk about with no built in cameras. Smart watches are slightly different - some have a camera in-built. Most rely on a close connection to the smart phone – an Apple Watch, for example, has a remote viewfinder for the phone but will only take a picture if the phone is near. Most smart watches rely on the smart phone being in close proximity. Smart watches should;

- Not be used to take pictures/video of any young people
- Not to be used to communicate with any young people
- Not be used in certain areas of the school e.g. areas designated as teaching spaces for pupils or used in school day.
- Most devices, Fitbits included, will send message notifications from phones. Staff must not read or reply to any messages during lessons or when working with children. Smart watches can be put into a "do not disturb" or "airplane" mode - this means that emails, text messages etc do not come through.
- ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.

School Provided Mobile phones, personal devices and all electronic devices with imaging and sharing capabilities.

- Where the school provides mobile phones, personal devices and all electronic devices with imaging and sharing technologies such as, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- All devices taken out of school should be password protected in case of loss or theft. Any photos or notes taken on the device should be uploaded to the school server / cloud W / One Drive.

Photographs and Video

- Digital photographs and videos are an important part of the learning experience in Green Park School and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

- As photographs and videos of pupils and staff are regarded as personal data in terms of GDPR 2018 we must have written permission for their use from the individual or their parent/carer. In our school, we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance.
- We seek written consent from parents/carers and staff who may appear in the media. Parental/carer permission is obtained annually. Parents/carers and staff are aware that full names and personal details will not be used in any digital media, particularly in association with photographs.
- The use of videos and cameras is not permitted in school, unless by an authorised member of staff with school equipment and for school purposes.
- When taking photographs/videos, staff ensures that pupils are appropriately dressed and are not participating in activities that could be misinterpreted.

Storage of Images

- Images/films of children are stored on the Evidence for Learning App.
- Staff **are not permitted** to use portable media storage of images (e.g. USB sticks).
- Rights of access to this material are restricted to the teaching staff within the confines of the school network

CCTV

Green Park uses CCTV for security and safety. The only people with access to this area are the Head Teacher and the Site Manager.

Laptops/iPads/Tablets

Staff Use:

- Where staff have been issued with a device (e.g. setting laptop) for work purposes the settings laptop/devices should be used by the authorised person only.
- Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will ensure that setting laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted and this must be acknowledged.

Children's Use:

- Laptop and iPad use must be supervised by an adult at all times and any games or apps used must be from a pre-approved selection checked and agreed by the Headteacher.
- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.
- Evidence for Learning allows staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs, videos and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork.

Personal staff mobile phones, personal devices and all electronic devices with imaging and sharing capabilities, should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.

Data Storage and Security

In line with the requirements of the GDPR, sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be accurate; secure; fairly and lawfully processed; processed for limited purposes and in accordance with the data subjects rights; adequate, relevant and not excessive; kept no longer than necessary; and only transferred to others with adequate protection.

At Green Park we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this eSafety policy. ICT enables efficient and effective access to and storage of data for the management team, staff and administrative staff.

The school complies with LA requirements for the management of information in Schools. We currently use SIMS on the school's administrative network. Only trained and designated members of staff have authority and access rights to input or alter data.

The school has defined roles and responsibilities to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided.

The computer network within the school has security against access to the management system. The files and network system are backed up daily so that copies of the data will always be available. Backup is managed by Eservices or a member of Senior Management (School Technician). This is done every evening. EServices ICT or a member of Senior Management also checks that the backup is working properly.

Approved anti-virus software is updated regularly on all Equipment (I-pads/smartboard/laptops etc) by L Russell or a member of Senior Management. All laptops and computers are password protected. All work email accounts are password protected. A secure email facility is available for staff that need to send confidential information. Passwords should be easy to remember, but hard to guess. Staff should not share their passwords with anyone; write their passwords down or save passwords in web browsers if offered to do so. Staff should not use their username as a password. Staff should not email their password or share it in an instant message. Staff should change their password if they think someone may have found out what it is.

Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the Head. Sensitive information should only be sent via the secure email system. Don't assume that third-party organisations know how your information should be protected.

The use of unencrypted memory storage devices to store information of a personal sensitive or confidential nature is not permitted.

Staff should only download files or programs from trusted sources. If in doubt, advice should be sought from L Russell or a member of Senior Management. If you are concerned that the email is suspicious do not open the email, seek advice from IT technician or open a ticket in the eservices reporting link and wait for their response.

Staff should lock sensitive information away when left unattended. Unauthorised people should not be allowed into staff areas. Computer screens should be positioned so that others who should not have access to that information cannot read them. Computer screens should be locked when the adult using it leaves his or her desk. Confidential documents should not be left out.

Staff should only take information offsite when authorised and only when necessary. On occasions when this is necessary, staff should ensure that the information is protected offsite in the ways referred to above. Staff should be aware of their location and take appropriate action to reduce the risk of theft. Staff should ensure that they sign out completely from any services they have used, for example email accounts. Staff should try to reduce the risk of people looking at what they are working with. Laptops should not be taken abroad (some countries restrict or prohibit encryption technologies).

Serious Incidents

If a serious incident occurs such as inappropriate content is accessed, the school concern report is completed immediately, a nominated officer is informed and appropriate action is taken until our technician (Eservices ICT or a member of Senior Management) has checked and ensured that the pathway is blocked.

Useful Links

Data Protection and Freedom of Information advice: www.ico.org.uk

Incident Reporting

Any eSafety Incident is recorded via the school Safeguarding Referral system so that all incidents can be given immediate attention and dealt with by the appropriate skilled team.

