Grangetown Primary School

Online Safety Policy

What is Online Safety?

- Online Safety encompasses not only direct internet access via PCs, laptops, or tablets, for example, but also electronic communications and web access via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people, and adults, about the benefits, risks & responsibilities of using online information technology.
- Online Safety is about safeguarding children and young people in the digital world.
- Online Safety emphasises learning to understand and use new technologies in a positive way.
- Online Safety is less about restriction and more about education about the risks as well as the benefits so that we can feel confident online.
- Online Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

Aims of this Policy

The aims of this policy are to set out the ways in which the school will:

- Build both an infrastructure and culture that supports Online Safety, ensuring that risk is minimised, and that staff and children are safe when using technology;
- Educate all members of the school community about their rights and responsibilities linked to the use of technology;
- Work to empower the school community to use technology including the Internet as an essential tool for learning.

Date of Policy & arrangements for Review

- This Policy was reviewed in July 2020.
- The next Review is set for July 2022 (unless there are curriculum changes in the interim).

Links with other GPS policies

This Online Safety Policy is used alongside other school policies, in particular the Child Protection & Safeguarding Policy and Acceptable Usage Agreements (see Appendices to this policy).

Contents

1. Roles and Responsibilities

Role	Responsibilities
Governors	• Approve and review the effectiveness of the Online Safety Policy • Online Safety will be reviewed by the DSL and Safeguarding governor
Headteacher	• Ensure that all staff receive suitable CPD related to Online Safety • Create a culture where staff and learners are able to report incidents • Ensure that there is a system in place for monitoring Online Safety • Follow correct procedures in the event of a serious Online Safety allegation being made against a member of staff or children • Inform the Local Authority about any serious Online Safety incidents • Ensure that the school network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented
Online Safety and Computing Leader and Designated Safeguarding Lead	• Monitor concerns logged by staff and inform others of Online Safety incidents, in conjunction with the Designated Safeguarding Lead • Lead the establishment to review Online Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety • Ensure that children are educated in Online Safety
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand, sign & follow the Acceptable Usage Agreements • Act in accordance with the Online Safety Policy • Follow the school's reporting procedure to report any suspected misuse or problems to the Designated Safeguarding Lead • Follow Child Protection procedures for all serious concerns • Monitor technology use in lessons, extracurricular and extended school activities • Plan appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum (in liaison with the ICT & Computing Coordinator, & the DSL)
Children	• Read, understand and sign the agreed school Acceptable Usage Agreement • Participate in Online Safety activities, follow the SMART rules and report any suspected misuse • Understand that following the SMART rules protects them out of school, including time spent on electronic devices • Support their friends to use the Internet responsibly and safely
Parents and Carers	• Endorse (by signature) the Child Acceptable Usage Policy • Discuss Online Safety issues with their child/ren and monitor their home use of technology devices (including mobile phones and games devices) and the Internet • Keep up to date with issues through newsletters and other opportunities • Inform the HT of any Online Safety concerns that relate to the school
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible • Create password protected accounts for staff members (so that confidential pupil information remains secure) • Maintain and inform the Senior Management Team of any issues relating to filtering, and/or of any breaches in terms of proper & safe internet use.
Visitors	• Use digital devices only in line with their business and in areas where they have been approved to do so • Do not take/use images of pupils unless approved to do so • Do not leave equipment unattended • Do not use digital devices belonging to the school unless approved to do so

2. Communicating and Disseminating this Policy

2.1 How the policy will be introduced to pupils

This will be taught through the Computing programme of study and as part of PSHE. Ongoing issues will also be covered in school newsletters and through assemblies and workshops.

- All users will be informed that network and Internet use will be monitored.
- An Online Safety programme of study (included in the bespoke curriculum planning documents for all year groups) will be established across the school to raise the awareness and importance of safe and responsible Internet use amongst pupils.
- Pupil instruction regarding responsiblity and safety.
- Online Safety rules will be posted throughout school.
- Safe and responsible use of the Internet and digital technology will be reinforced across the curriculum

2.2 How the policy will be disseminated to staff?

It is important that all staff feel confident to use new technologies in teaching and the Online Safety Policy will only be effective if all staff subscribe to its values and procedures. ICT use is widespread and all staff including administration, midday supervisors, governors and volunteers will be included in awareness raising and training. Induction of new staff will include a discussion about the school Online Safety Policy.

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement, and regularly review the Acceptable Use Agreements.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user and that any misuse will be addressed in line with school procedures.
- Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The school will highlight useful online resources which staff should use with children in the classroom.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Disciplinary action could be taken if they are found to bring the profession or school into disrepute.

2.3 Gaining the support of Parents & Carers

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school will help parents plan appropriate, supervised use of the Internet at home and educate them about the risks.

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, on the school website and also through regular awareness raising workshops.
- A partnership approach to Online Safety at home and at school with parents will be encouraged. This will include offering parental workshops with resources, links and suggestions for safe home Internet use, or highlighting Online Safety at other attended events (e.g. class assemblies, parent workshops and productions).

3 Teaching and learning of Online Safety

3.1 Why Internet use is important

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions as well as maintaining an online presence to the wider community.
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

3.2 How Internet use benefits education

Benefits of using the Internet in education include:

- Access to worldwide educational resources
- Educational and cultural exchanges between pupils worldwide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to educational materials
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with Sunderland City Council and DfE;
- Access to learning wherever and whenever convenient

3.3 How Internet use can enhance learning

- Staff should guide pupils to online activities that will support the learning outcomes planned for pupils' age and ability.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- The school will ensure that the copying and subsequent use of internet-derived materials by staff and pupils complies with copyright law.

3.4 How pupils learn how to evaluate Internet content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research internet content.

4 Managing Information and Data Systems

4.1 How information systems security will be maintained

- Virus protection for the whole network is installed and current. Files held on the school's network will be regularly checked.
- Unapproved software will not be allowed on any device.
- The Network Manager will review system security regularly.

4.2 How email will be managed

- All staff will be issued with an 'official' school email, with password protected access
- If email contact with parents is required, the generic 'office' email account should be used (via office staff or HT), rather than a 'named' account.
- Staff must immediately tell a designated member of staff if they receive offensive email, or if they find and 'spam' emails with inappropriate content.

4.3 How published content will be managed

- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- Pupils' personal information will not be published.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

5 Digital Video and Images

5.1 How the use of digital images and videos will be managed

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images and videos on the internet.

- Written permission from parents/carers will be obtained before images/videos of pupils are electronically published online. The main vehicles for this are the school website and social media accounts (Twitter, Instagram, Facebook), but can also include approved third parties (visits, visitors, local press etc).
- When taking digital images and posting on school website and school social media accounts (Twitter, Instagram, Facebook), staff should view this as an opportunity to model good practice with regards to the appropriate use of social media.
- Staff are allowed to take digital video/images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without adult permission.
- Pupils' full names must not be used anywhere on the school website or Twitter account. First names can be used in text only posts, but no child should be made identifiable by associating names with videos or images.

6. Social Networking

The rapid emergence of new technologies has brought about the opportunity to communicate with others in a variety of new ways. Increasingly, technology has become a vital part of both our working and our social lives and, when used responsibly, it can be a positive tool to enhance teaching and learning. However, as with many new developments, the widespread use of social networking sites has implications for schools and for school staff. It is important that as an educational establishment, we preserve our good reputation and meet our legal responsibilities regarding social media.

6.1 Our Aims in terms of social media

We will ensure that employees' use of social networking sites:

- Enhances student learning where appropriate (e.g. school Twitter account).
- Serves to maintain the positive working relationships which exist in school.
- Does not reduce our ability to effectively safeguard pupils.
- Does not expose individuals or the school to potential legal action.
- Does not bring the name of the school into disrepute.

6.2 Definition of 'social networking sites'

For the purposes of this policy, the term 'social networking' refers to any websites or apps which allow individuals to interact with others, by sharing information, opinions, knowledge, interests, pictures, video clips or photographs. This includes sites such as Facebook, Instagram, Snapchat and Twitter but also covers other web-based services including podcasts, blogs, wikis and video sharing sites such as YouTube.

Our social media procedures apply to all staff who work at our school. This includes teachers at all levels of responsibility, supply staff, support staff, including part time support staff, governors, volunteers, and external service providers who work with our pupils and contractors.

6.3 Our Expectations

Employees are personally responsible for the information they choose to publish online. Our school encourages its entire staff to take care in protecting their privacy and that of the school, our pupils and their families.

The school regards all e-communications as being within the public domain, given that no one has control of the content once it is sent. In the light of this, online activities should reflect the same levels of respect, consideration, honesty and professionalism that a colleague would use in person and this should be consistent with the standards and expectations outlined in the DFE's 'Teaching Standards' document. Similarly, personal views expressed concerning non-school issues should not be in conflict with our school's ethos and expectations. Racist or homophobic comments, for example, would be considered unacceptable on the basis that at as school we do not tolerate discriminatory attitudes.

6.4 Social networking during the school day

Social networking for purely social purposes should not take place during teaching and learning time, and should be confined to an employee's designated break or lunch time. Where social networking sites are being used for educational purposes (e.g. school Twitter account), this may take place at other points in the school day, but it is expected that individuals posting items or information will have gained permission to do so from the Headteacher. Those with permission to post to the school's social media accounts will have previously agreed to adhere to a set of school standards (included within this policy document).

6.5 Identifying oneself as an employee of our school

In identifying oneself as an employee of our school on a social networking site, an individual is automatically viewed as a representative of the school. This means that everything posted on to that individual's page has the potential to reflect on the school and our image. Any employee naming the school also takes on the responsibility of representing the school in a professional manner and must therefore ensure that their profile and related content is consistent with how they wish to present themselves to colleagues, parents and pupils as well as being consistent with the image and ethos of the school

6.6 References to school based issues and stakeholders

Discussions of school-based matters should be undertaken with caution. If an employee does express a view on a school-based matter, it is important that the employee makes it very clear that the view does not represent that of the school itself.

Care must also be taken in making reference to other staff, pupils, parents, governors or any other member of our school community. Our relationship with our stakeholders is crucial and could be damaged through the making of ill-considered comments. Pupils in particular should not be referred to by name and negative comments about members of our school community should not be made. Images of colleagues should not be placed onto any online site without first gaining permission from that colleague. Images of colleagues should be removed immediately upon their request. If a colleague has any doubt about the appropriateness of a comment or posting, they should err on the side of caution. It is important to remember that posts are archived online and cannot be permanently deleted.

6.7 Confidential information

As a school, we often legitimately need to discuss confidential information with colleagues. This type of information should not be discussed or referred to, even implicitly, on social networking sites. This includes discussions on private messaging sections of these sites, which are not guaranteed to be a secure form of communication.

6.8 Online ‘links’ with pupils/parents/ex pupils

It is our policy that employees do not become online ‘friends’ with current or ex-pupils on social networking sites, and that staff do not ‘follow’ these individuals or groups. This measure is designed to maintain professional boundaries, and provide protection against possible inappropriate online behavior.

6.9 Posting of videos or photographs of pupils

Videos, photographs or any other images of pupils should not be posted online without first having received signed authorisation from the parents/guardians. In all circumstances, images which identify pupils as being members of our school should only be used with extreme care. Names are never linked to photographs.

6.10 Copyright and other legal issues

Employees must comply with the law with regard to copyrights and plagiarism. The work of others should not be posted on sites without permission unless it is in the form of brief quotations, which comply with ‘fair use’ exceptions. Employees must also consider their legal position with regard to libel and defamation of character. Writing defamatory statements can result in legal action, brought by the victim. Furthermore, the school may take its own action if it feels an employee has brought the school’s name into disrepute.

6.11 Conclusion

Our school is keen to embrace emerging technologies, such as social networking sites. Our aim is not to discourage this use but merely to ensure that all of our school community, both staff and pupils, remain safe while doing so. Our approach seeks to ensure that staff are well informed, and confident in their ability to protect themselves and our pupils.

7. Technical Infrastructure

The School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements

- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and the data held on our server.
- All of our systems are protected by up to date virus software, by filtering systems and by a range of other security protocols.

Access to the school network and Internet is carefully controlled and well-secured:

- Users having clearly defined access rights to school ICT systems through group policies
- Adult users being provided with a username and password
- Children/classes being provided with a username/log-on
- Users being made aware that they are responsible for the security of their usernames and passwords and must not allow other users to access the systems using their log on details
- Users must immediately report any suspicion or evidence that there has been a breach of security
- An agreed process being in place for the provision of temporary access for visitors e.g. supply teachers, training providers, etc, onto the school system.

The Internet will be controlled with regard to access controls, which fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites, through an automated 'key word' system, whereby dynamic content filtering examines web page content or email for unsuitable words.
- URLs are auto-monitored for inappropriate results; rating systems give each web page a rating for sexual, profane, violent or other unacceptable content, and these ratings are used to restrict access where necessary.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate access.

The ICT systems of the school will be monitored with regard to:

- The school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems
- Online Safety incidents being documented and where appropriate reported immediately to the Designated Safeguarding Lead, who will arrange for these to be dealt with immediately in accordance with the Acceptable Usage Policy

It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using the Internet and that Acceptable Usage Agreements are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online and should recognise acceptable and unacceptable behavior, and be aware of a range of ways to report concerns about content.

It is worth noting at this point that we have never experienced any failures in our internet security systems at Grangetown. No inappropriate content has ever 'gotten through'. This does not mean that our systems are beyond failure, of course, but does demonstrate how effective the systems

are at blocking inappropriate content. Despite this, we will never be complacent – we will remain constantly vigilant.

Any material that the school believes is illegal must be reported to appropriate agencies such as Sunderland City Council, Police/CEOP.

Websites which schools believe should be blocked centrally should be reported to ConnectEdIT technical staff. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc just before the lesson. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age & maturity of pupils.
- The school will work with ConnectEdIT to ensure that filtering policy is continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Designated Safeguarding Lead who will then record the incident and escalate the concern as appropriate.
- The school's ICT Support provider will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Sunderland City Council, Police or CEOP.

8. Anti (Online) Bullying Policy

8.1 Introduction

It is a Government requirement that all schools have an Anti-Bullying policy. The Grangetown Policies are available here:
https://grangetown.sunderland.sch.uk/docs/Policies/Updated_policies_2019-20/Anti_Bullying_Policy_Updated_Jan_2020.pdf
https://grangetown.sunderland.sch.uk/docs/Policies/Updated_policies_2019-20/Childrens_Anti-Bullying_Policy.pdf

8.2 Online Bullying

Online Bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone" (DCSF 2007).

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, social media, gaming or the Internet, they can often feel very alone and vulnerable, particularly if the adults around them do not understand online bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how online bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident internet users will support raising awareness and keeping people safe.

Online Bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- There are clear procedures in place to support anyone in the school community affected by Online Bullying.
- All incidents of Online Bullying reported to the school will be recorded.

- There will be clear procedures in place to investigate incidents or allegations of Online Bullying under the Bullying Policy
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to online bullying and the school's Online Safety ethos.

Sanctions for those involved in Online Bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

8.3 Monitoring and review

Our Anti-Online Bullying Policy is monitored on a day-to-day basis by the Deputy Headteacher and Headteacher, assisted by our ICT & Computing Subject Leader. We report to governors on a termly basis, regarding the effectiveness of the policy.

9. Mobile Devices: Staff / Pupils

Staff are allowed to bring mobile phones into school but they must only use them during break, lunchtimes or during non-contact when they are not in contact with children unless they have the permission of the Headteacher. The devices must be turned off or onto silent during the school day. Staff are not allowed to use personal devices to take photographs or videos in school.

Staff should not use their personal mobile devices to contact children, parents and carers.

On school trips, staff may use a personal mobile phone to contact school, if necessary. If any contact is needed with parents, that should be via the school office.

Children who bring mobile phones into school should hand them to their class teacher at the start of the day and then collect them again at the end of the school day. Parental permission is required for this, and the parent should also state a reason (in writing) why the phone is being brought into school. Pupils are not permitted to use mobile phones at any point during the school day.

10. Policy Decisions

10.1 How Internet access will be authorised

- All staff will read and sign School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

- Pupils will use age-appropriate online resources and these will be teacher-directed where necessary.

10.2 How risks will be assessed

- The school will take all reasonable precautions to ensure users access only appropriate material. In part, this is linked to the setting of appropriate guidance (see Acceptable Use policies), and to ensuring that all users are educated in correct internet use. It is also linked to the systems that have been put in place by our highly trained technicians – e.g. anti-malware software, firewalls, and thorough filtering procedures – they will be monitored weekly, and updated as appropriate (in response to technological advances, for example).
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 - breaches will be reported to Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

10.3 How the school will respond to any incidents of concern

Online Safety risks can be experienced unintentionally, or deliberately by people acting inappropriately or even illegally.

We encourage pupils to report issues and concerns immediately. In addition, staff are trained to recognise the signs that some form of inappropriate use may be going on (e.g. online bullying). Staff know that any such concerns must be reported immediately, to the Designated Safeguard Lead.

Staff and pupils should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Any inappropriate activity would need to be reported to the school Designated Safeguard Lead.

Where there is cause for concern or fear that inappropriate or illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. Assuming that the Headteacher is not the subject of concern, a decision to escalate would normally sit with the Headteacher. The decision to involve Police should be made as soon as possible, after contacting the Children's Safeguarding team, if the offence is deemed to be out of the remit of the school to deal with. Staff should however be encouraged to take matters further if they are NOT satisfied with leaders' responses.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, Online Bullying, illegal content etc).
- The Designated Safeguarding Lead will record all reported incidents and actions taken in the incident log. Any Online Safety incidents involving Child Protection concerns will be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learned and implement any changes required.
- Where there is cause for concern or fear that inappropriate or illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team and escalate the concern to the Police

10.4 How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher

- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.

10.5 How is the Internet used across the community?

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the Internet and technology whilst on the school site.
- In accordance with the Computing programme of study, the school will educate children on how to use technology safely and respectfully, impacting on school, home and community behaviour.

11. Acceptable Usage Agreements

The school will ensure that staff and visitors will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for children and will, in return, expect staff and visitors to agree to be responsible users.

The Acceptable Usage Agreements apply to staff and visitors who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

The following Acceptable Use Agreements are in place and are attached for reference to this policy:

- Staff Acceptable Use Agreement
- Staff iPad Acceptable Use Agreement
- Staff Laptop Acceptable Use Agreement
- Visitor Agreement (including acceptable usage of digital devices)
- Parent and Carer Acceptable Use Policy
- Children's Acceptable Use Policy (SMART Rules)

Grangetown Primary School - Acceptable Use Agreement for Staff

The school will ensure that staff and visitors will have access to the internet, to facilitate efficient and effective working, and to enhance learning opportunities for children, and will, in return, expect staff and visitors to agree to be responsible users.

This Acceptable Use Agreement applies to staff and visitors who have access to and are users of school ICT systems and to school-related use of ICT systems outside of school.

Responsibilities

I agree to:

- Follow the School Online Safety policy.
- Report any suspected misuse or problems to the Headteacher or Deputy Headteacher
- Monitor ICT activity in lessons, extracurricular and extended school activities.
- Model the safe use of ICT.
- Refrain from publishing any information that may be offensive to colleagues, may breech the integrity of the ethos of the school or may bring the school into disrepute.

Education

I understand that I am responsible for the Online Safety education of children.

- I will respect copyright and educate the children to respect it as well.

Training

- I understand that I will participate in Online Safety training.
- I understand that it is my responsibility to request training if I identify gaps in my knowledge & skills.

Online Bullying

- I understand that the school has a zero tolerance of bullying. In this context online bullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures.

Technical Infrastructure

I will not try to by-pass any of the technical security measures that have been put in place by the school.

Passwords

I will only use the password(s) given to me.

- I will never log another user onto the system using my login.

Filtering
I will not try to by-pass the filtering system used by the school.

- If I am granted special access to sites that are normally filtered, I will not leave my digital device unsupervised.
- I will report any filtering issues immediately.
- I understand that the school will monitor my use of digital devices and the Internet.

Data Protection
I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.

- I will ensure that all data held in personal folders is regularly backed up.

Use of digital images
I will follow the school's policy on using digital images making sure that:

- Only those children whose parental permission has been given are published.
- Full names of pupils are not used
- Personal devices are not used to capture any images.

Communication
I will be professional in all my communications and actions when using school ICT systems.

Email
I will use the school provided email for all school-related email communication

- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Personal publishing
I will follow the Online Safety policy concerning the personal use of social media.

Mobile Phones
I will not use my personal mobile phone during contact time with children.

- I will not use my personal mobile phone to contact children or parents.

Reporting incidents
I will report any suspected misuse or problems to the Deputy Head/Designated Safeguarding Lead.

- I will follow Child Protection procedures for all serious concerns.
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary procedures
I understand that there are regulations in place when children use ICT and that there are sanctions if they do not follow the rules.

- I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

I have read, understood and agree to abide by the terms of the Staff Acceptable Use Policy.

Name: _____

Signature: _____ Date: _____

Headteacher's signature: _____ Date: _____

Grangetown Primary School - iPad Acceptable Use Agreement

Staff should aim to bring their iPad to school every day, fully charged; this is because: (i) the iPad calendar & email are important tools in the school's communication systems, and (ii) so that the device can be used to demonstrate good practice with children, to take photographs, or – for example – to use the Early Years assessment and observation software (Tapestry).

All iPad users will be required to read this AUP and sign it. They will also agree to follow all relevant procedures, be role models, and demonstrate good practice in the use of these devices.

Staff will be provided with an iPad, USB Cable, USB Charger and case. The iPad must be passed back to the school in appropriate working condition, on termination of employment or at the request of the Headteacher. Grangetown Primary School reserves the right to require the return of an iPad from a staff member at any time and without notice.

At all times the iPad shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and email. Individual users are responsible for the setting up of any home Internet connection to use in conjunction with the iPad.

Maintenance and Care of Devices

- Staff issued with an iPad are expected to exercise the same care in respect of the security and upkeep of the iPad as if it were the employee's own property.
- Malfunctions or any other technical problems (either hardware or software related) should be reported to the Headteacher, so that steps can be taken to have the problem rectified by an approved technician as quickly as possible.
- Staff should be aware that insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home but excludes theft from your car or from other establishments. If the iPad is lost or damaged as a result of neglect on behalf of the staff member, then you may be responsible for a contribution towards the replacement of the device.
- The iPad screens are particularly sensitive to damage from excessive pressure on the screen. Users must avoid placing too much pressure and/or weight (such as folders and workbooks) on the screen in order to refrain from any unnecessary damage. It is recommended that the supplied cases are used, including the protective sleeves.
- The iPad must not be subjected to extreme heat or cold.
- Users must take responsibility for installing software updates (updates provide important security settings and it is therefore essential that these are installed). If you need assistance with this, our on-site technicians can help.
- Users must keep the iPad clean and in good working order.

Security and Privacy

- Users should secure their iPad with a confidential password (for assistance, see technicians).
- It is a good idea to activate the 'Find my iPad' function – again our ICT Coordinator or one of our technicians can assist. This allows a missing iPad to be located via the iCloud.
- It is a user's responsibility to keep their iPad safe and secure. When iPads are left unattended they must be stored in a safe place around school.
- It is a user's responsibility to ensure that their allocated iPad is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the iPad in a communal area, any off-site venue and whilst travelling.
- iPads must not be left unattended or on view in motor vehicles at any time.

- If the iPad is lost, stolen or damaged, please notify the Headteacher. If necessary, the device will be remotely locked and/or wiped. Grangetown Primary School is not responsible for the loss of any personal files that may be deleted remotely from an iPad.
- The use of 'Jailbreaking' is strictly prohibited ('Jailbreaking' is the process which removes any limitations placed on the iPad by Apple, resulting in a less secure device).
- You must ensure that your school email account has been enabled on your iPad and that you have checked email prior to the start of each school day. This is a key means of communication for staff, and is therefore essential that you check your email account on a regular basis.
- You must ensure that the school shared calendar is enabled on the iPad calendar app, and checked daily, as this is a key means of communication of events within school.
- As well as the Acceptable Use Policy, staff must adhere to the Data Protection Act (1998), the Computer Misuse Act (1990) & the GPS Health and Safety Policy, when using iPads in school.
- When using iPads with pupils it is your responsibility to ensure that children are not accessing confidential information.
- Users may not use private emails to send content that, if intercepted, would place the school in violation of laws or regulations.
- Staff may not use the Internet to view illegal or inappropriate material that would place the member of staff or school at legal risk.

Applications

- You have the ability to download apps which you feel may be of benefit to you, or your pupils.
- Upon receiving an iPad, staff will be provided with an iTunes card, to enable you to install the school's 'core apps'.

Social Media

- For the purposes of this policy, social media includes (but is not limited to) Internet forums, blogs, wikis, podcasts, photograph websites (Flickr, Instagram, Snapchat, etc.), Facebook and Twitter. Staff should follow these guidelines in relation to any social media applications that they use, both in work and in their personal lives.
- Users should not access social media applications from the school's iPads when working in school unless it is for educational purposes (e.g. school Twitter account).
- Users should understand that anything they write (regardless of privacy settings) could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.

Use of Digital and Video Images

- Staff using iPads must be aware of the risks associated with sharing images & videos online.
- Users must make good judgment when using the iPad camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Staff must not take, use, share, publish or distribute images of others without their permission.
- Inappropriate media may not be used as a screensaver or background photo.
- Deletion of photos and videos may be necessary, from time to time, if a iPad memory is full.

I have read, understood and agree to abide by the terms of the iPad Acceptable Use Policy.

iPad Serial Number:_____

Name: _____

Signature: _____ Date: _____

Headteacher signature:_____ Date: _____

Grangetown Primary School - Parent and Carer Acceptable Use Agreement

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet.

The Internet will be used within school to support children's learning. Children will be taught to be critical in their use of Internet sites.

As a parent or carer, you will agree to:

- Endorse (by signature) the Child Acceptable Usage Policy
- Discuss Online Safety issues with your child/ren and monitor their home use of technology devices (including mobile phones and games devices) and the Internet
- Keep up to date with issues through newsletters and other opportunities
- Inform the Headteacher of any Online Safety concerns that relate to the school

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, on the use of the Internet at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on future access to school facilities.

If you do not understand any part of this document, you should ask a member of staff for guidance.

This form below must be completed, signed and returned to the school for our records.

Parent's name	
Child's name	
Class	
Date	
Comments	

Grangetown Primary School - Children's Acceptable Use Agreement

- Technology is an amazing resource to support your learning in school and at home. It can also be a great way to communicate with others.
- Your school wants to make sure that you use technology in a safe way.
- All children at Grangetown have discussed online safety with their teachers (in an age appropriate way), and have agreed to follow the rules set out below.

My Responsibilities

- I understand that I have rights and responsibilities in using ICT and will act responsibly when using technology, digital devices or the Internet. WE have discussed what this means with our teacher.
- I will only use the user names and passwords I have been given
- If I bring a mobile phone into school, I will hand it to my class teacher upon entering school and collect it again at the end of the school day.
- I will learn the school's SMART rules to keep myself safe inside and outside of school
- I will report any suspected misuse or problems to a teacher or trusted adult within school.
- I will make sure there is permission to use any material that I find (i.e. copyright). Again, we have discussed this with our teacher.

Communication – (eSchools, email, Twitter, blogging, Skype etc.)

- I will be careful in my communications making sure that nothing I write is offensive, and that it is considerate.
- I will not write anything that could be seen as insulting to the school.

Online Bullying

- I understand that the school will not accept bullying in any form, including online bullying.
- I will be careful with all communications making sure that anything I write is considerate and could not be interpreted as bullying.
- I understand that I should report any incidents of bullying.

Childs Name	
Signature	
Class	
Date	

BE SMART ONLINE

Childnet International

S – SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M – MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

THINK U KNOW

A – ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R – RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T – TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**

BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

WWW.CHILDNET.COM