



Garfield Primary School

Online Safety Policy

Shared with staff in September 2017

Ratified by Governors – Autumn 2017

Introduction

Garfield Primary School recognises that the use of ICT is expanding rapidly in all sectors of society from internet technologies to electronic communications such as mobile phones and wireless technology. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial. The internet is vast and unregulated, and, in common with all communication media, there remains however the concern that it can be abused. Therefore this policy sets out strategies for the safe and responsible use of the School network and the internet.

All users are accessing the internet both in and out of the School. Therefore Garfield aspires to ensure that all users in school are aware of potential risks and how to practise safe, responsible behaviour whenever and wherever they are online. The School's online safety policy will work alongside with other policies that we have in place at Garfield including those for curriculum, bullying, data protection, security and pupil behaviour.

We want all users of technology to be safe online when they are in our care and to educate them to protect themselves when they are not in our care so that when they use technology that is new to them, they act in a responsible and safe way.

We want all professionals to use technology to enhance their practice and find new ways of personalising learning to suit the different aptitudes and interests of learners, including those with special needs. Technology can improve the planning and delivery of teaching as well as making the learning experience more dynamic and interactive. ICT can help to ensure learners find the learning process more meaningful, enjoyable and engaging. Therefore, we want the effective use of technology to be embedded in teaching and learning across all of the School's activities.

Contents

Policy Objectives

Statement of Responsibilities

Responsibilities of Staff

Responsibilities of the School Leadership team, in liaison with the Computer Science Subject Leader and the ICT Technician at the School:

Responsibilities of the Computer Science Subject Leader and ICT Technician

Internet access in school

Ensuring internet access is appropriate and safe

Media Publications

Use of School Cameras

Social Networking Sites (SNS), Newsgroups, and Forums, Chat and instant messaging, Personal Website and Blogs

Maintaining the security of the school ICT network

Using the internet to enhance learning

Using information from the internet

Using e-mail

Garfield Primary School Website

E-Safety and home/school links

Policy Objectives

Garfield Primary School's policy is to protect users within the School, so far as is reasonably practicable, from harm, whilst maximising the educational and social benefits from using technology. Therefore, this policy aims to give guidance on how this is to be accomplished.

Statement of Responsibilities

Garfield Primary School has a responsibility to ensure that all reasonable and appropriate steps have been taken to protect users whilst using Information Technologies.

Responsibilities of Staff

Although all staff have a responsibility to exercise a duty of care, it is important that staff are aware of their specific obligations with regard to Online Safety.

All staff are responsible for their own actions and the use of ICT facilities by them at the School. The School assumes and implies compliance with this policy without exception.

All staff should be familiar with current policies, standards and legislation relating to the use of the internet, apps and technology.

All staff should comply with the security measures laid down in this policy. Abuse of the computer network, apps or the internet, may result in disciplinary action, including possible termination of employment and civil and / or criminal liability.

All staff should ensure they know how this policy relates to all other related Garfield Primary School, e.g. Anti Bullying and the implications of the use of ICT in their classes.

The person responsible for safeguarding students should also have responsibility, together with the ICT Technician, to review online-safety in the School on a regular basis, at least twice every academic year.

Responsibilities of the School Leadership team, in liaison with the Computer Science Subject Leader and the ICT Technician at the School:

Make the Online Safety Policy to all staff available on the Staff shared drive;

Ensuring **all staff** are aware of the Policy;

Maintaining online-safety procedures appropriate to the information systems in use;

Keep accurate records of all staff and students who are granted internet access. These records will be kept up-to-date, with such as a member of staff leaving or the withdrawal of a student's access.

Ensuring all inappropriate use of technology is appropriately dealt with and their occurrence is monitored.

Responsibilities of the Computer Science Subject Leader and ICT Technician

The development of the Garfield Primary School Online Safety Policy.

To review this Policy regularly in the light of ever-changing technologies

Providing the necessary software tools and security utilities to maintain the integrity and confidentiality of the School systems e.g. use of up to date virus scanning software

Ensuring security systems, firewalls, virus scanning software (where appropriate) are up to date

Internet access in school

Providing access to the internet, apps and online platforms in school will raise educational standards and support the professional work of staff.

Teachers and pupils will have access to web sites world-wide (including museums and art galleries), applications and online platforms offering educational resources, news and current events, as well as e-books and maths resources. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

In addition, staff will have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LEA and DfES; receive up-to-date information and use online resources such as the LGFL, Bugclub, Skoolbo and many more.

In the longer term the internet may also be used to enhance the school's management information and business administration systems.

Staff, including supply staff, will not be expected to take charge of an internet activity without checking they are trained. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the internet, will be provided with the School Online Safety Policy, and will have its importance explained to them.

Parents' attention will be drawn to the Policy by letter in the first instance and, thereafter, in our school prospectus and on our school website. Our school Online Safety Policy will be available for parents and others to read on demand.

Ensuring internet access is appropriate and safe

Some material available on the internet is unsuitable for pupils. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet.

However, taking into account the size and amount of content on the internet along with the fact that the vast majority of sites are unregulated, it is almost impossible to provide completely safe access for children. Whilst we can endeavour to protect children online at school, many children will have internet access at home via a computer, laptop, phone, tablet and games console or now even by smart T.V's with unrestricted internet capabilities some older children may have smart watches that still can access the online world. Social networking websites are very popular with children and even though they are not permitted at school large numbers use them (inappropriately) at home. The dangers of these sites are not always apparent and children need to be made aware of them. It is, therefore, just as important to teach children how to be safe online as it is to provide them with access that is as safe as we can make it.

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet access is purchased from the LGfL which provides a service designed for pupils including a "firewall" filtering system intended to prevent access to material inappropriate for children;
- Children using the internet will normally be working in the ICT room or their classrooms, during lesson time and will be supervised by an adult (usually the Computer Science teacher if in that subject) at all times;
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;
- Pupils will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others this will only take place in KS2;
- Our Rules for Responsible Internet Use will be posted near computer systems.
- The Computer Science Subject Leader will monitor the effectiveness of internet access strategies;
- The Computer Science Subject Leader will ensure that occasional checks are made on files to monitor compliance with the school's Online Safety Policy;
- YouTube is blocked to all children in the school including the app on the tablets.
- The Head Teacher will have overall responsibility to ensure that the policy is implemented effectively;
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advise from the LEA, the LGfL and the DfES.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. *Neither the school nor Enfield Council can accept liability for the material accessed, or any consequences thereof.*

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the Computer Science Subject Leader and the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher. All the teaching staff will be made aware of the incident in *Pupil Awareness* at a Staff Meeting if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue;
- If staff or pupils discover unsuitable sites the Computer Science Subject Leader and technician will be informed. The Computer Science Subject Leader will report the URL (address) and content to the Internet Service Provider and the LEA; if it is thought that the material is illegal, after consultation with the ISP and LEA, the site will be referred to the Internet Watch Foundation and the police.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use which have been designed to help protect them from exposure to internet sites carrying offensive material. If pupils abuse the privileges of access to the internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to the internet may be denied for a period.

Media Publications

Video and photographic technologies can be very powerful learning tools. However, photographs and/or video may be taken by staff to support educational aims only. Named images of students will only be published with the separate written consent of their parents or carers. Publishing includes, but is not limited to:

Web broadcasting,

TV presentations

Newspapers

Care should be taken when capturing photographs or videos to ensure that all students are appropriately dressed and permissions gained from parents and carers in line with normal guidance.

Student's work will only be published if the parent's or carer's written consent is received. This may be altered or amended at any time by the parent or carer by written request.

Use of School Cameras

To ensure the safety of pupils only school cameras should be used to photograph pupils and the media should only be filed on either the class computers or the School Network. Personal mobile phones should not be used to take photos or video of pupils

Social Networking Sites (SNS), Newsgroups, and Forums, Chat and instant messaging, Personal Website and Blogs

Please see Social Networking appendix

Expectations of Staff with respect to use of Social Networking Sites (SNS)

It is **NOT** acceptable for staff to make pupils/ex-pupils 'friends',

Staff will not discuss School issues on the site,

No photos connected to school are to be posted on SNSs,

Privacy settings are strongly advised to be set 'friends only',

Staff should not use SNS in school hours.

Maintaining the security of the school ICT network

We are aware that connection to the internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The Computer Science Subject Leader and ICT Technician will install the Sophos antivirus software that has been purchased by the LGfL on all computers in the school. This software automatically updates and will deal with any currently known virus quickly. Staff computers will also have this software installed and staff will be able to access automatic updates at home.

The Computer Science Subject Leader will give yearly INSET to staff to ensure that they are fully aware of network security and are able to use the software effectively.

Using the internet to enhance learning

Pupils from Year 1 onwards will learn how to use a web browser and applications. Older pupils will be taught to use suitable web search engines and applications. Staff and pupils will begin to use the internet to find and evaluate information. Access to the internet and applications is a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet and applications will be used depending upon the nature of the material being accessed and the age of the pupils:

- access to the internet may be by teacher (or sometimes other-adult) demonstration;
- pupils may access teacher-prepared materials, rather than the open internet;
- pupils may be given a suitable web page or a single web site or an application to access;

- pupils may be provided with lists of relevant and suitable web sites and applications which they may access;
- Older, more experienced, pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher; pupils will be expected to observe the Rules of Responsible Internet Use and will be informed that checks can and will be made on files held on the system and the sites they access.

Pupils accessing the internet or applications will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet or applications once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the internet.

Using information from the internet

We believe that, in order to use information from the internet effectively, it is important for pupils to develop an understanding of the nature of the internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited or edited and most of it is copyright.

- pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium);
- when copying materials from the Web, pupils will be taught to observe copyright;
- pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using e-mail

Pupils will learn how to use an e-mail application and be taught e-mail conventions. Staff and pupils will begin to use e-mail to communicate with others, to request information and to share information.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use and the reasons for these rules.
- teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- pupils may send e-mail as part of planned lessons but will not be given individual e-mail accounts at present;
- in-coming e-mail to pupils will not be regarded as private;
- children will have the e-mail messages they compose checked by a member of staff before sending them;
- the forwarding of chain letters will not be permitted;

- pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

Garfield Primary School Website

Our school web site is intended to:

- provide accurate, up-to-date information about our school;
- enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- celebrate good work;
- provide pupils with the opportunity to publish their work on the internet;
- promote the school.

Publish letters and resources for planned homework projects

All classes may provide work for publication on the school web site. Class teachers will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status.

The Computer Science Subject Leader will be responsible for up-loading pages to the school web site, ensuring that the links work and are up-to-date, and that the site meets the requirements.

The point of contact on the web site will be the school address, telephone number and e-mail address.

Each year parent's permission will be sought for the use of pupils' names and photographs and filming that identify individuals on our web pages. A Child's full name will never be used and home information or individual e-mail identities will not be published either. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

School website address: <http://www.garfield.enfield.sch.uk>

Online Safety and home/school links

Parents will be informed in our school prospectus that pupils are provided with supervised internet access as part of their lessons. We will keep parents in touch with future ICT developments by letter and newsletter.

Internet use in pupils' homes is rapidly increasing and some parents may be grateful for any advice/guidance that school can offer – especially with regard to safe access for children. The Computer Science Subject Leader is willing to offer advice and suggest alternative sources of advice on the understanding that neither he/she, the school nor the LEA can be held responsible for the consequences of such advice. Further:

- school guidelines on issues such as safe internet use will be made available to parents together with printed information and internet sites providing information for parents about safe access for children;

- the Computer Science Subject Leader will offer demonstrations/practical ICT sessions for any parent who requests it so to inform and encourage a partnership approach;
- Suitable educational and leisure activities that make responsible use of the internet are available to parents or carers through the website.

As noted above, it is not possible to be certain of the originator of an e-mail message, and for this reason the school is unable to accept an e-mail as parental authorisation of a pupil absence.

Appendices

Appendix 1 Social Networking Guidelines for All School Staff

1.0 Introduction

- The Governing Body of Garfield Primary School is committed to ensuring that all school staff are aware of their responsibilities in connection with the use of social networking sites. It recognises that the use of such sites has become a significant part of life for many people. They provide a way of keeping in touch with friends and colleagues, and can be used to exchange ideas and views on common interests. Examples of such sites include, but are not limited to, Facebook, YouTube, MSN, Google Hangouts, Forums, Bulletin Boards, Twitter, Chatrooms and instant messenger, Instagram, Snap Chat, WhatsApp etc.
- Staff are expected to maintain a professional distance from pupils and therefore staff should not be involved in social networking with pupils either in or outside of school - including past pupils. If this is not adhered to it will be seen as a 'child protection issue'.
- Whilst it is important that staff are able to use technology and related services effectively and flexibly, they must ensure that, when doing so, they do not make themselves vulnerable. This must also be balanced with the duty of the Headteacher and the Governing Body to safeguard children and the reputation of the School and the Council.

2.0 Scope

- This policy will apply to all staff in this school whose contracts of employment have been issued by the Local Authority on behalf of the Governing Body or by the Governing Body itself.
- It will also apply to supply staff employed by agencies, and any breach of the policy by supply staff will result in the supply arrangement for that particular worker being terminated and matters reported to the employment agency.

3.0 Aims

- The policy aims to:
 - a) Reinforce the need to use social networking sites safely and securely;
 - b) Ensure that staff are aware of the risks associated with the inappropriate use of social networking sites;
 - c) Safeguard staff in connection with the use of social networking sites and to ensure they do not put themselves in vulnerable situations;
 - d) Ensure that the Headteacher, the Governing Body and all staff maintain their duty to safeguard children, the reputation of the school and the reputation of the Council.

4.0 Responsibilities

- The Governing Body:
 - a) Must ensure that this policy is implemented.
 - b) Must ensure that both current and new employees have access to, and are made aware of, this policy.
- Headteacher:
 - a) Must be fully aware of this policy and ensure that they and all other teaching and support staff are aware of the policy and their own responsibilities.
 - b) Must ensure that staff have been made aware of the risks of using social networking sites and the possible implications to their employment if there is inappropriate use.
 - c) Should seek advice where necessary from Human Resources.
 - d) May need to instigate disciplinary procedures.
- Employees:
 - a) Must behave responsibly and professionally at all times in connection with the use of social networking sites.
 - b) Must follow this policy.
 - c) Must co-operate with the School's management in ensuring the implementation of this policy.
- Human Resources:
 - a) Will provide advice and support to the Headteacher, the Governing Body and the School's management in relation to this policy.

5.0 Use of Social Networking Sites

- Staff should be aware that when communicating via social networking sites anything said, shown or received could be made available, intentionally or unintentionally to a wider audience than originally intended. Therefore staff must follow the procedures below:
 - a) Staff **must not** access social networking sites for personal use via school information systems or using School equipment.
 - b) Staff **must not** accept pupils/students as 'friends' and must not approach pupils/students to become their friends on social networking sites. Such personal communication could be considered inappropriate and unprofessional.
 - c) Staff **must not** befriend pupils who have previously attended Garfield Primary School and are under the age of 18 years.
 - d) Staff **must not** post inappropriate photographs (including photographs of pupils) on any social network site.
 - e) Staff **must not** post any indecent / defamatory / racist or sexist remarks.
 - f) If a member of staff receives messages on his/her social networking profile, which they think, could be from a pupil they must report this to the Headteacher, who will decide the appropriate action.
 - g) Staff, **must not** make any reference to their place of work or their profession with an educational environment. This includes reference to the location of their profession or use of images that can link to an educational establishment (e.g. photos including school logos).
 - h) Staff **must not** disclose, on any social networking site, any information that is confidential to the School, Governing Body or the Council or disclose any personal data or information about any individual/colleague/pupil, which may breach the Data Protection Act.

- i) Staff **must not** disclose any information about the School/Governing Body or the Council that is not yet in the public arena.
- j) Staff **must not** make defamatory remarks about the School/colleagues/pupils, the Governing Body or the Council or post anything that could potentially bring the School, Governing Body or Council into disrepute.
- k) Staff **must not** disclose any confidential information relating to his/her employment at the School.
- l) Staff **should** take care to avoid using language or images, which others could deem as offensive or unprofessional.

6.0 Breaches of the Policy

- Although the School/Governing Body does not discourage staff from using social networking sites, all staff should be aware that the Headteacher/Governing Body will take seriously any circumstances where such sites are used inappropriately, including any usage that is considered to be online bullying or harassment.
- The Headteacher can exercise his/her right to monitor the use of the School's information systems, including internet access, where s/he believes unauthorised use may be taking place; to ensure standards are maintained; to prevent or detect crime and to pick up messages when someone is away from school. If such monitoring detects the unauthorised use of social networking sites disciplinary action may be taken.
- If any instances or allegations of the inappropriate use of social networking sites are brought to the attention of the Headteacher, investigations will take place and disciplinary action may be taken.
- Any breach of this policy may constitute an act of gross misconduct.
- There may be instances regarding the use of social networking sites where the School, Governing Body or the Council will be obliged to inform the police of any activity or behaviour about which there are concerns as to its legality.

7.0 Further Guidance

- As professionals having daily contact with pupils/students, any contact on such sites with young people who may be friends of pupils/students is inappropriate.
- It is advised that staff do not accept parents of pupils in their school as 'friends' on social networking sites. This has to be a personal judgement. If this is felt to make a member of staff vulnerable they should remove the 'friend'
- If there are special circumstances relating to 'friends' being parents this needs to be discussed with the Headteacher.
- If staff accept parents as 'friends' on social networking sites they must follow the rules of this policy in relation to professional conduct, implications of inappropriate words, images and usage.
- Instances or allegations of inappropriate use in relation to social networking with parents of pupils will be investigated and may lead to disciplinary action.

8.0 Equality Statement

- This policy must be applied fairly to all employees irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

Appendix 2

Rules for Responsible Internet Use

The school has installed computers with Online-Safety to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

- I will only access the computer system with the login and password I have been given;
- I will not access other people's files;
- I will not bring in CD Roms or USB Flash Drives from outside school and try to use them on the school computers.

Using the internet:

- I will ask permission from a teacher before using the internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

Using e-mail:

- I will ask permission from a teacher before checking the e-mail;
- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I receive or send may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will only send an e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.

Appendix 3

Garfield Primary School

Upper Park Road,
New Southgate,
Enfield,
N11 1BH,

Dear Parents/Carers,

Use of the Internet and E-mail

As you may know, it is government policy that all schools connected to the internet so that pupils and teachers will be able to exchange electronic mail with partner schools and search for information from museums, libraries, news providers and suitable web sites related to their lessons.

There have been widely publicised concerns about pupils having access to undesirable materials when they use the internet. We believe that the educational advantages of enabling the children supervised access the internet greatly outweigh the likely problems if appropriate safeguards are put in place. We have purchased our internet access from the London Grid for Learning (LGfL), an educational supplier which operates a filtering system to block access to inappropriate materials. Our computer screens will be in public view and, as stated above, internet access will be supervised.

The school has prepared a detailed Online-Safety Policy which is intended to help us make the most of the opportunities that the internet offers whilst minimising the possible risks. It includes a set of Rules for Responsible Internet Use that we will be teaching the children and I attach a copy of these.

We regret that, because it is not possible to be certain of the originator of an e-mail message, the school is unable to accept an e-mail as parental authorisation of a pupil absence.

Should you wish to read our school Online-Safety Policy or to discuss any aspect of internet use please telephone me to arrange an appointment.

Yours sincerely,

ICT Subject Leader