

Glenleigh Park Primary Academy

E Safety & Media Policy

Approved by: Governing Body

Date Approved: May 2017 at LAB Meeting

Date for Review: May 2018

Contents

- Acceptable Use Statement
- Staff Password Policy
- Teacher Laptops
- Data In Transit
- Contact with pupils
- Internet Access Policy Statement
- Internet
- E-mail
- Video Conferencing Or Similar Interactive Learning Technologies
- Managing emerging technologies
- Pupils
- Social networking and personal publishing
- Internet use at home
- Internet and System Monitoring
- Internet Publishing Statement
- Use of Portable Equipment
- Assessing Risks
- Handling E-safety complaints
- Glenleigh Park Primary Academy Procedures
- Appendices

Acceptable Use Statement:

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences; or allow adults to enhance their own professional development.

The school recognises that technologies such as the Internet and e-mail will have a profound effect on children's education and staff professional development in the coming years and the school's Internet Access Policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use.

Staff Password Policy:

Staff are required to use "strong" passwords when accessing the school network or learning platform. Passwords should contain a mixture of letters, numbers and punctuation characters. Staff must not share passwords, must not log on and allow anyone else to use the workstation and must ensure that if a workstation is left unattended, it is locked. (Using Ctrl/Alt/Del and selecting "Lock Workstation").

Staff Laptops:

Staff laptops, or other devices assigned to staff by the school must only be operated by them. It is inadvisable to permit family members or anyone else to operate the equipment. Staff using laptops at home need to ensure they have adequate insurance in place. Staff should adhere to the school internet access policy statement when using school laptops at home.

Data In Transit

It is recognised that teachers need to hold and share a large amount of data pertaining to pupils. The Data Protection Act (1990) requires that all data is held securely, accessed only in

accordance with the provisions of the Act and transferred in a secure manner. To transfer data from school to home staff must use encrypted memory sticks. Staff must under no circumstances create and keep “local” copies of data on workstations or their own personal computer systems or USB memory keys.

Contact with Pupils:

Staff should only have contact with pupils online via school technologies e.g. class email address / through the Learning Platform’s messaging and forums. Staff should not add pupils past or present as friends on social networking sites such as Facebook. Staff are reminded that, while respecting the privacy of personal social networking sites, there should be nothing there that might bring the profession into disrepute.

Internet Access Policy Statement:

All Internet activity should be appropriate to staff professional activities or the children’s education. It has been drawn up to protect all parties; the students, the staff and the school.

Internet:

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person or written down;
- The Internet may be accessed by staff and children throughout their hours in school;
- Activity that threatens the integrity of the school’s computer systems, or that attacks or corrupts other systems, is prohibited e.g. knowingly allowing a virus onto the system. If a deliberate activity contrary to the intentions of this policy results in damage to the school systems, recompence may be sought.
- All Internet activity should be appropriate to staff professional activity or the pupil’s education. Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise school use e.g. staff may use internet to access personal e-mails outside of directed time.
- Use of the school’s Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school’s network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights.

- All web activity is monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task.

- Users accessing inappropriate materials should expect to have their permission to use the system removed.

Email:

- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media. Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.

- No data covered by the Data Protection Act (1990) may be sent in an unencrypted format via email.

- Posting anonymous messages and forwarding chain letters is forbidden;

- Downloading attachments to emails should only take place where you have requested these attachments and are therefore certain of their origin.

- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden and may lead to disciplinary action being taken or involvement of outside agencies.

- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

- It is advisable for staff to use their school email account as opposed to personal e-mail accounts for school based work. Our school "signature" is placed at the end of all e-mails.

- Children are not to be given individual e-mail addresses in school. Teachers may set up whole class e-mails but these must be strictly monitored by the class teacher.

Video Conferencing Or Similar Interactive Learning Technologies:

- Video Conferencing will be booked in advance between schools or through a trusted provider under the strict supervision of school staff.

- Ensure video conferencing equipment is switched off when not in use and not set to auto answer.

- Ensure that video conferencing contact information is not put on the School Website.

- Ensure that parents and guardians have given express consent for their children to take part in video conferences.
- Ensure that only staff are issued with unique log on and password details for educational videoconferencing services.
- Ensure that all sites and participants have given written permission in advance when recording a videoconference lesson. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Ensure that recorded material is stored securely.
- Ensure that, if third-party materials are included in the lesson, it is acceptable to do so to avoid infringing the third party intellectual property rights.

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed (with effect to new technologies emerging after Sept 2016).
- Pupil's mobile phones must not be used during lessons or formal school time. Pupils should hand in their mobile phone to office staff for the duration of the school day. Teachers and TAs may use their mobile phone during the school day for activities which enhance the children's learning (e.g. checking calendars or setting stop watches.)
- The sending of abusive or inappropriate text messages is forbidden.

Pupils:

- Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult;
- The teaching of e-safety is included in the school's computing Scheme of Work, but all teachers within all year groups should frequently be including e-safety issues as part of their discussions on the responsible use of the school's computer systems;
- All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off or close the laptop lid and report immediately to a member of staff.

Social networking and personal publishing:

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, and may well breach the conditions of the site (eg minimum age of 13 on BEBO or Facebook).

Internet use at home:

- Parents and Carers will be advised to contact their own Internet Service Providers to explore home filtering and child controls.
- Parents are advised not allow their child unsupervised access to the internet.
- Parents should be advised to visit the e-Safety section of the school website or Learning Platform for further information on e-Safety at home.

Internet and System Monitoring :

Through Smooth Wall all Internet activity is monitored. If it is suspected that there are any transgressions of the school's Internet policy and/or use of obscene, racist or threatening language detected by the system the ICT team can request logs of dates and times of internet sites visited. Occasionally, it may be necessary for the ICT team to investigate attempted access to blocked sites, and in order to do this, the ICT team will need to set his/her Internet access rights to "Unrestricted". Whenever this happens, this should be recorded in the ICT incidents register, and the Headteacher notified. (NB – the ICT team includes the computing subject leader / technicians / ICT working party) All serious transgressions of the school's Internet Access Policy are recorded in the school's ICT Incident register. The Incident register can be found on the 'J:' drive. Transgressions of Internet Policy and use of inappropriate language can be dealt with in a range of ways, including for pupils removal of Internet access rights; computer system access rights; meetings with parents or even exclusion; in accordance with the severity of the offence and the school's Behaviour Policy. Breaches of Internet Access Policy (found within this document) by staff will be reported to the Headteacher and will be dealt with according to the school's and LEA's disciplinary policy, or through prosecution by law.

Internet Publishing Statement:

The school wishes the school's web site and Learning Platform to reflect the diversity of activities, individuals and education that can be found at Glenleigh Park Primary Academy. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent.
- All photos published on the schools website and learning platform must only be of minimal resolution to view on screen.
- No names of children are to be used on the school's website or any school run social media site.
- No link should be made between an individual and any home address (including simply street names);
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not (for example is it a piece of un-named artwork or a photograph of the child).
- Photographs remain the property of the school and must not be kept in any form. As such they must be removed from home based PCs, laptops and other forms of data storage when suitably formatted for the purpose intended.
- Photographs are taken for the sole purpose as stated below and may not be used by any individual for their own business or other interest.

Use of Portable Equipment:

The school provides portable ICT equipment such as laptop computers, colour printers and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities. Exactly the same principles of acceptable use apply as in the Acceptable Use Statement above.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the computing co-ordinator;
- Certain equipment will be stored centrally. Once equipment has been used, it should be returned to the storage area;
- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy and that the equipment is fully insured from the moment it leaves the school premises. Computing

equipment is not to be left in cars as this is not secure and is unlikely to be covered by any insurance policy.

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;
- If an individual leaves the employment of the school, any equipment must be returned;
- Staff should not install software on the laptops or computers without the express permission of the computing subject leader.
- The use of USB sticks, external HDDs etc. is permitted but staff should run regular anti-virus software checks.

Assessing risks:

- The school will take all reasonable precautions to ensure that users access only appropriate material.
- However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ESCC can accept liability for the material accidentally accessed, or any consequences of Internet access.
- The school will audit computing provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints:

- Complaints of Internet misuse will be dealt with initially by the e-Safety Coordinator or a member of the SLT if e-safety coordinator is not available.
- All e-Safety incidents will be recorded in the format shown in appendix E. This is known as the 'e-Safety Incident Record.
- A copy of the e-Safety Incident Record will be sent to the headteacher, the Child Safety Officer, ESCC. One copy will be stored in the pupil or staffs file. One copy will be kept by the e-Safety Coordinator.
- Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.
- Discussions may be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- E-safety incident flow chart displays the course of action taken as shown in appendix D.

Glenleigh Park Primary Academy School Procedures:

The school has developed a set of guidelines for Internet use by KS2 pupils. [Appendix A1] A simplified 'poster' is offered for KS1 pupils. [Appendix A2] These rules will be made available to all pupils, and kept under constant review. Parents' permission is requested for children to have Internet access at school. [Appendix B] This request also covers whether a child's image may be used as part of the school's website under the guidelines of our website policy. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils. All members of staff are shown this policy at either staff training sessions or during induction and are expected to follow guidelines established for their own Internet use. Staff and other adults who are asked to take photographs of pupils on behalf of the school for use on the website, prospectus etc. must sign a declaration of agreement for the safe use of such material. [Appendix C]

Appendix A1

General

Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.

Access to the Internet is provided for pupils to conduct research and communicate with others. Parents' permission is required.

Access is a privilege and requires the user to act responsibly. Computer storage areas and USB flash drives will be treated as school property. Staff may review files and communications to ensure that users are using the system responsibly.

Guidelines

- All Internet activity should be appropriate to the student's education
- Access should only be made via the authorised account and password, which should not be made available to any other person;

The following are not permitted:

- Use of the network to access inappropriate materials such as inappropriate, racist or offensive material.
- Posting anonymous messages and forwarding chain letters.
- Activity that threatens the integrity of or damages the school ICT systems or activity that attacks or corrupts other systems.
- Use for personal financial gain, gambling, or political purposes or advertising.
- Sending or displaying offensive messages or pictures, using obscene language, harassing, insulting or attacking others.
- Breaking copyright laws
- Using others' passwords
- Trespassing in others' folders, work or files
- Intentionally wasting resources

Consequences

Breaking the above rules will result in a temporary or permanent ban on Internet use. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour. When applicable, police or local authorities may be involved.

Appendix A2

Using the internet at Glenleigh Park.

- Always ask a teacher before using the internet.
- Only visit websites you have been told you can use.
- If you see something that makes you feel uncomfortable turn off the computer and tell your teacher immediately.
- Keep your passwords safe!

Appendix B

Internet and Photograph Parent Permission Form

Dear Parents & Guardians,

At Glenleigh Park Academy we love to celebrate your child's work and achievements through different media. We also highly value the academic opportunities provided by the internet and email in the modern learning environment. Please read through the following statements and tick to show you give permission for each one.

If you have any concerns about any of these statements please speak to a member of the leadership team.

I give permission for my child to use electronic mail and the internet with adult supervision.

I give permission for my child's photograph/video to appear on the school's website, the school's Facebook Page and Learning Platform under the strict guidelines set up by the school.

I give permission for my child's photograph to appear in the local newspaper, magazines and other non-school publications.

I give permission for the Academy to use quotes, work etc. completed by my child on the school's website and the Facebook page and learning platform.

Please note:

- children will not be given their own email address - whole class emails will be used exclusively,
- we will never publish a child's name alongside their photograph,
- children will be allowed to contact one another through the school's learning platform. This is monitored by the class teacher,
- Internet access is only granted when supervised by an adult and internet safeguards are in place.

Name of pupil..... Class.....

Parent/Guardian name Signature



Appendix C

Glenleigh Park Primary Academy

Using images and video safely on school websites

This signed declaration is for the use of those who are involved with taking or using images of pupils for the purpose of promoting the school through the website, prospectus or other school events. Due to recent legislation and concerns over the safeguarding of pupils please read, sign and return this sheet to school.

- Photographs remain the property of the school and must not be kept in any form. As such they must be removed from home based PCs, laptops and other forms of data storage when suitably formatted for the purpose intended.
- Photographs are taken for the sole purpose as stated below and may not be used by any individual for their own business or other interest.

I agree with the above statements and will adhere to them accordingly

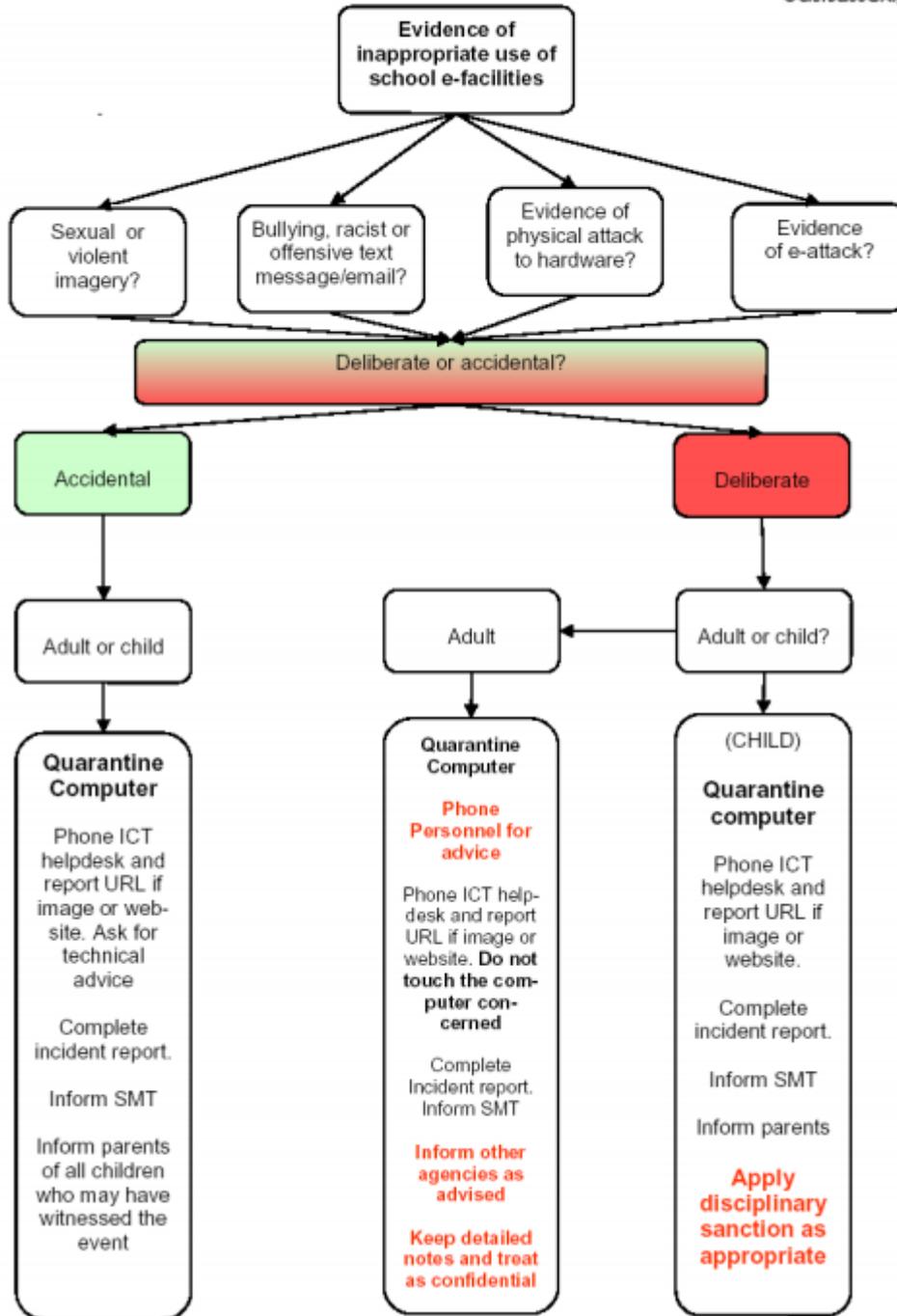
Photographs taken / used by

For the purpose of

Signed

Appendix D

E-safety incident guidance for staff



Appendix E

Date & Time					
Reporting staff name					
Name of children (or adults) involved in the incident					
Nature of incident (circle)	Accidental access to inappropriate material	Intentional access to inappropriate material	Cyber bullying	Grooming	Other
Details					
The event occurred (circle)	During a lesson	Outside school hours	Outside of a lesson	Unsupervised access	
Police involvement required?	Grooming	Violent images	Pornographic images	Other criminal activity	
Parents contacted (date , time and details)					
Further actions					

