# Online Safety and Acceptable Use of ICT Policy

## Giles Brook School

GILES BROOK SCHOOL

| | | |
|---|---|---|
| **Written by:** | Jenny Brown | **Date:** 21/03/2017 |
| **Last Reviewed On:** | 19/03/2019 | **Policy Number**: E2 |
| **Next review due by:** | 01/03/2020 | |

| | |
|---|---|
| **ICT Coordinators** | Sam Hawkes ( Phase 2 )<br>Claire Dinsey ( Phase 1 and Foundation ) |
| **Online Safety/Designated Safeguard Lead** | Debbie Williamson |
| **This policy has been written in conjunction with keeping children safe in Education (2016 - with a particular focus on Appendix C) Giles Brook child protection policy and safeguarding procedures.** | |

## Contents


1. Introduction Page 3
2. Roles and Responsibilities Page 3-4
3. Online Safety in the Curriculum Page 4
4. Pupils with Additional Needs Page 4
5. Email Page 4-5
6. Online Safety Support for Staff Page 5
7. The Internet Page 5-6
8. The Taking of Images and Film Page 6
9. Publishing Pupils' Images and Work Page 6-7
10. Storage of Images Page 7
11. Webcams and CCTV Page 7
12. Video Conferencing Page 7
13. Personal Mobile Devices Page 7
14. Parental Involvement Page 7-8
15. Security Page 8
16. Server Security Page 8
17. Using Removable Media Page 8
18. Monitoring Page 8
19. Breaches Page 8
20. Incident Reporting Page 9
21. Protecting Personal, Sensitive, Confidential Information Page 9
22. Viruses Page 9
23. Disposal of ICT Equipment Page 9
24. Zombie Accounts Page 9
25. Use of Twitter within School Page 10
26. Use of Facebook for School account Page 10
27. School YouTube Account Page 10


**Appendices**


A. Acceptable Use Agreement for Pupils and Parents Page 11
B. Acceptable Use Agreement for Staff Page 12
C. Acceptable Use Agreement for Governors Page 13
D. Acceptable Use Agreement for Parent Helpers / Volunteers / Work Experience Students Page 14
E. Social Networking Sites & Personal Internet Presence for School Staff Page 15-16

## 1 Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

As 'Keeping Children Safe in Education' - 2016 states:

*The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:*

- *content: being exposed to illegal, inappropriate or harmful material;*
- *contact: being subjected to harmful online interaction with other users; and*
- *conduct: personal online behaviour that increases the likelihood of, or causes, harm.*

Our school policy has the main aim of addressing these areas of risk.

Information and Communication Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies that children and young people are using, both inside and outside of the classroom, include:

- Websites
- Email, instant messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile / Smart phones with apps, text, video and / or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning platforms and virtual learning environments
- Computer programming
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not constantly policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements, usually 13 years.

At Giles Brook, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

All staff will have attended basic GDPR training and they must make sure they have read and are familiar with the following policies which are part of the General Data Protection Regulation:

- Data Protection Policy (GDPR)
- Information Management Toolkit For Schools - Still under development
- Privacy Notice Staff

## 2 Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Assistant Headteacher is the online safety coordinator who has been designated this role and works alongside the ICT co-ordinator and IT technician. All members of the school community have been made aware of who holds this post.

The Assistant Headteacher updates the senior leadership team and the governors, so that they have an understanding of the issues and strategies at our school, in relation to local and national guidelines and advice.

This policy, supported by the school's 'Acceptable Use Agreements' for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Social Networking, Safeguarding, Health and Safety, Behaviour (including anti-bullying) and PSHE.

## 3 Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety. We teach age-appropriate issues following national and local guidelines so that our pupils can be using online resources safely from Nursery right through to Year 6.

- The school provides opportunities within a range of curriculum areas to teach about online safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the online safety curriculum.
- Social networking sites will not be used, although pupils will be educated in their safe use.
- Pupils are aware of the relevant legislation when using the Internet, such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information and protecting their own personal information, safe use of images and other important areas through discussion, modelling and appropriate activities.
- Online safety rules will be posted in all rooms where computers are used and are discussed with pupils regularly.
- Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or the CEOP 'Report Abuse' button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- Pupils are taught to guard themselves against grooming of all kinds, with an emphasis on not trusting all strangers online.
- We participate in local and national online safety promotions.

## 4 Pupils with Additional Needs

The school endeavors to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's online safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children and young people.

## 5 EMail

The use of email within school is an essential means of communication. In the context of school, email should not be considered private. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette ('netiquette'). In order to achieve expected attainment in ICT, or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business, as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business. (Google can be contacted if emails have been deleted.)
- Confidential information to be shared with external agencies via email will be sent/received using an encrypted email system such as Egress.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school accounts on the school system and only under direct teacher supervision for educational purposes.
- Emails created or received by staff as part of their job, will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their email account as follows:
  - Delete all emails of short-term value.
  - Organise email into folders and carry out frequent housekeeping on all folders and archives. Sensitive emails or those which need keeping for a long period of time, should be saved to Google drive or the server in an organised file structure, so that the mails can be easily located.

- Never open attachments from an untrusted source.
- Keep the number and relevance of email recipients.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive, rather than sending attachments.

- Pupils are introduced to email as part of the ICT Scheme of Work.
- Children have their own individual school issued google account.
- The forwarding of chain letters is not permitted in school.
- All pupil email users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Emails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, emails should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email, whether directed at themselves or others and before it is deleted.
- Staff must inform the online safety coordinator if they receive an offensive email, whether it is directed at themselves or others and before it is deleted.
- However members of the school community access their school email account, whether directly, through webmail when away from the office or on non-school hardware, all the school email policies apply.
- School email accounts are not to be used for personal use, advertising, or registration for any personal use..
- The automatic forwarding and deletion of emails is not allowed.
- The school reserves the right to monitor any Giles Brook email account at the discretion of the headteacher or online safeguarding lead.
- Staff can only have access to the Google suite on their personal mobile devices as per the Mobile Device Management Policy.
- All staff are NOT permitted to access any private email accounts on a school device, inside or outside of school.

## 6 Online Safety Support for Staff

- Our staff receive regular and appropriate information and training on online safety and how they can promote the 'Stay Safe' online messages. This is usually through the usual scheduled programme of staff meetings.
- New staff receive information on the school's 'Online safety and Acceptable Use Policy' as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of technology misuse by any member of the school community.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas.
- The whole school takes part in Safer Internet Day annually.

## 7 The Internet

The Internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up using the GBS Child Protection Policy. The school will take reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor the schools broadband supplier can accept liability for any material accessed, or any consequences of Internet access.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher (e.g. Espresso). It is advised that parents check these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Online gambling or gaming is not allowed.
- All staff, volunteers and governors must also comply with the ***'Social Networking Policy'*** ( appendix E ) regarding the posting of any information or images relating to the school.
- School Internet access is controlled through E2BN Protex proxy filtering system. The filtering system is updated by E2BN with all the latest protection, which includes keywords associated with terrorist, extremism and radicalisation. The school has the ability to block any websites they choose on top of what E2BN supply.
- As a school we do not over block websites, we do constantly teach children what to do in the event they do see something that makes them feel uncomfortable. In the ICT suite they will press hector to blank the screen and then tell an adult.

Laptops / ChromeBooks they close the lid. iPads they turn screen down. At home, minimise then go and tell an adult. They know not to close the page, so that the inappropriate site can be reported to the IT technician to take action to stop it happening again.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the online safety coordinator or teacher as appropriate. There is a CEOP button on the school website which pupils can use (when in school or at home) to report abuse or inappropriate websites. 'Hector the Dolphin' button is used on school computers so that children can instantly block their screen if they have seen something inappropriate.
- Protext filter monitoring. The school has access to basic log files which are monitored randomly by the IT Technician to check for access to content.
- The school does not have an automated monitoring system in place, the policy to ensure absolute protection is physical monitoring. Pupils are NOT allowed access to the internet unsupervised by an adult.
- If any inappropriate material has been accessed then Giles Brook safeguarding procedures / policy will be followed.
- Giles Brook is aware of its responsibility when monitoring staff communication under current legislation.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- It is the responsibility of the school, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- It is every member of staff's responsibility to shut down their computer every evening to allow updates to run.
- Pupils and staff are not permitted to download programs on school based technologies without seeking prior permission from the ICT Technician.
- If there are any issues related to viruses or anti-virus software, the ICT technician should be informed.
- The school does not allow any access to social networking sites whilst on the school premises. This does not include the school Twitter account, which is used for educational purposes.
- Youtube is allowed in school but everyone using it is made aware of how inappropriate content may appear and searches should be done before sharing with the children, whenever possible.
- No access or searches should be made to any illegal website.
- The school uses Google Apps for education which allows full control over any user access to the internet, including email, youtube, google drive, calendar, classrooms and sites. All functionality can be switched off for any user.
- Staff laptops and ipads will be subject to random checks to ensure appropriate use.

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks and how to manage these risks.

## 8 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff and visitors are not permitted to use **personal** digital equipment, such as mobile phones and cameras or iPads, to record images of pupils, this includes when on field trips. Appropriate images can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted from the individual device.
- Photographs and videos may be taken by parents/carers during specified school events to which they have been invited such as a school play. Parents must be made aware before, or at the start of the event, that images must be for private use only and cannot be uploaded to social media sites.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.
- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS checks and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.
- When students go on school trips, permission to take photos at the event by the event organisers should be sought in writing from parents before the trip.

## 9 Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website, school twitter account.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded / transmitted on a video or webcam. Some films occasionally get put on the school YouTube channel
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.

- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. However, it is the practice of the school to ask parents to re-sign this at the beginning of each new key stage and parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

**10 Storage of Images**

- Images / films of children are stored on the school's google drive, school network or on school iPads and not on other personal portable storage devices (e.g., USB sticks), without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

**11 Webcams and CCTV**

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Staff must ensure webcams are switched off when not in use.
- CCTV is mounted in several locations around the school for security and protection.
- The CCTV images are backup to an onsite storage device and kept for 14 number of days.

**12 Video Conferencing**

- Permission is sought from parents and carers if their children are involved in video conferences, by the class teacher.
- All pupils are supervised by a member of staff when video conferencing is taking place..
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

**13 Personal Mobile Devices (including phones)**

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Children's mobile phones are to be stored in the class phone boxes at the start of each day in the office and collected by the child at the end of the day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The creation and/or sending of inappropriate messages, images (including pseudo images), videos or sounds between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- School mobile phones should be used by staff when out on a school trip.

Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- Cause harm,
- Disrupt teaching,
- Break school rules,
- Commit an offence,
- Cause personal injury, or
- Damage property.

Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them. Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy.

**14 Parental Involvement**

- Parents/carers are asked to read through and sign an Internet and email agreement on behalf of their child on admission

to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to online safety where appropriate in the form of:
    - Information evenings
    - Practical training sessions
    - Newsletter items
    - School Website – information, links to websites and copy of the policy

**15 Security**

The school gives relevant staff access to its Management Information System, with a unique username and password

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents, which include the '***Social Networking Policy'*** **( Appendix E )** and the Acceptable Use Agreement **( Appendix B )**
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it should be kept locked out of sight.
- Staff should always carry a portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control and out of sight at all times. (See Staff laptop, iPad home use agreement.)
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.
- All ICT equipment is security marked as soon as possible after it is received. The bursar maintains an audit log - FMS (on SIMS) to register of all ICT equipment and other portable assets.
- As a user the school ICT equipment, members of the school community are responsible for their own activity.
- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory.
- It is imperative that staff save their data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any data that is not held on the school's network.
- Staff must not save files onto the desktop as this will not be backed u and is a security risk..
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a time locking screensaver is applied to all machines. All staff must be responsible for locking their computer when left unattended. (Windows + L)
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, staff must return all ICT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- The installation of any applications or software packages must be authorised by the IT technician.
- Supply teachers have a separate log-on and teachers will make sure any resources are copied into 'Shared Documents'.

**16 Server Security**

- School servers are kept in a locked and secure environment and there are limited access rights to these which are password protected.
- Existing servers should have security software installed appropriate to the machine's specification and the school uses a remote backup service for SIMS data. Curriculum data is backed up daily, 2 fire doors away from the server room.

**17 Using Removable Media**

- No removable storage devices are allowed onto any school machine. Sophos is used to block this permission.
- Data should not be saved to CD or DVD unless permission is given by the head teacher and IT technician.

**18 Monitoring**

- Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, facsimiles etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).
- Internet activity is logged by the school's internet provider and in addition the school's technician will regularly monitor the websites which are accessed on school equipment.

**19 Breaches**

- If relating to Safeguarding, the Designated Safeguard Lead will be informed in the first instance and school policy procedures will be followed.

- Data breaches should be reported to the headteacher and IT technician immediately the **Data Protection Policy** should then be followed.
- A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.
- Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

## 20 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's online safety coordinator, headteacher and the IT Technician. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the IT technician / headteacher..

An incident log is used to monitor what is happening and identify trends or specific concerns. Any Safeguarding concerns are logged on CPOMS and the headteachers will be notified.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online safety coordinator.
- Deliberate access to inappropriate materials must be reported immediately to the Designated Safeguard Lead and, depending on the seriousness of the offence, will lead to further investigation by the Headteacher / LA, possibly leading to disciplinary action, dismissal and involvement of police for very serious offences.

## 21 Protecting Personal, Sensitive, Confidential and Classified Information

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access.
- Personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- The security of any personal, sensitive, confidential and classified information contained in documents which are faxed, copied, scanned or printed.
- Only download personal data from systems if expressly authorised to do so by the Headteacher.
- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
- Hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

They protect school information and data at all times, including any printed material.

## 22 Viruses

- All files downloaded from the Internet, received via email must be checked for any viruses using school provided anti-virus software before being used.
- We have banned removable media such as memory sticks from school.
- Never interfere with any anti-virus software installed on school IT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT technician.
- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact your IT Technician immediately.

## 23 Disposal of ICT Equipment

- All redundant IT equipment will be disposed of through an authorised agency.. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- Any redundant IT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be overwritten multiple times to ensure the data is irretrievably destroyed.
- All redundant IT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
- Disposal of any IT equipment will conform to current legislation and will conform with the governors' policy on the disposal of equipment.

## 24 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Technical staff will ensure that all user accounts are disabled once a member of the school has left.

**25 Use of Twitter within School**

Twitter is used at Giles Brook to assist the school with direct day to day communication with our parents and the wider community. It is an effective tool for staff to use to get instant messages to parents, share students success and share the day's events with those who follow the class page, the master twitter account or parents who look at the feed from the Giles Brook Website.

- The school has a master Twitter account @GilesBrookSCH which is looked after and monitored by the IT Technician.
- The Headteacher, Assistant Headteacher and Deputy Headteacher also have access to this account.
- The master twitter account is linked and embedded onto the first page of the school website and on the digital signage board in reception.
- Each class teacher, Headteacher, Deputy Headteacher, Assistant Headteacher, school office, breakfast club, sports coach, friends association have their own twitter account.
- The Master School account only follows school twitter accounts.
- When any school account tweets the master account is notified. The tweet should then be checked by the person who maintains the master account for relevance and security before it is retweeted onto the master account.
- Staff with a school / group account must ONLY use this account for school use. They must NEVER post any personal information or their own opinions on this account.
- Staff who have personal twitter accounts, should NEVER link to any of the school twitter accounts.
- The class account remains the property of the school and ownership will be passed back to the school when the teacher moves on.
- If a parent tags the school or class account in a tweet, the following rules need to be followed.
    - If a child's photo is uploaded by the parent and they put the child's name, the school must not respond or retweet that tweet.
    - The person responding or retweeting, needs to quickly check the validity and appropriateness of the account before doing so.
    - If a question is asked, answer the question without tagging the person who asked.

**26 Use of Facebook for School Account**

As per recommendations the school has set up a Facebook login using a school facebook email address. This is to secure the Giles Brook School name is owned by the school, so that nobody can pretend to be the school and set up a facebook account with our name. The IT Technician should termly check facebook search for Giles Brook / Giles Brook School and make sure that nothing is being posted under our name.

This dummy account is locked so that nobody can post on our wall. This is a dormant account until the headteacher / governors see fit to make it active.

**27 School YouTube Account**

The school has a youtube channel which is used to share the students work online. Searchable as:
Giles Brook Primary School

- The IT Technician is in control of the Giles Brook account and all movie uploads will go through them.
- Only students whose parents have signed the publication agreement can have their work published.
- No student must ever use their name when introducing themselves in a video or put their name in the credits.
- There are links from the school's website to the Youtube channel and new content will also be tweeted or embedded on the school website.
- Any comments left on our videos will get notified to the IT Technician who manages this account.

**Appendix B.** **Acceptable/Responsible Use Agreement and Safety Rules for Pupils and Parents/Guardians**

GILES BROOK SCHOOL

- I will only use ICT in school for school purposes.
- I will only use my class email address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not send photographs or videos or any other information about myself to others.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my online safety.
- Student access will be subject to random checks to ensure appropriate use.

**Pupil's Agreement**

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times. (Parents are asked to read and explain the rules for responsible use with their children.)

Signed:_____ Print name: _____ Class: _____

Date: _____

**Parent's/Guardian's Consent for Computer Use and Internet Access**

I have read and understood the school rules for responsible computer and internet use and give permission for my child to access the Internet. I have also read and understood the school's online Safety Policy (published on our GBS website). I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school or Milton Keynes Council cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Print Name: _____

Date: _____

**Appendix B.** **Acceptable/Responsible Use Agreement for Staff**

GILES BROOK SCHOOL

- I will only use the school's email, Internet, twitter, network and any related technologies for professional purposes or for uses defined as 'reasonable' by the Headteacher or governing body.
- I will ensure that personal data (such as data held on SIMs software) is kept secure and is used appropriately on school premises. Personal data can only be taken out of school when authorised by the Headteacher.
- No Memory sticks are allowed to be used by anyone on the school network.
- I will not install any hardware or software without permission of the Headteacher or ICT Technician.
- I am aware that I may use my school laptop for personal use, however I must ensure that at no time this is being used inappropriately or inappropriate material is being accessed – this includes any materials that could be considered offensive, illegal or discriminatory.
- I will ensure that my use of ICT is in keeping with the 'E-Safety Policy and Acceptable Use Policy', as well as the 'Social Networking Policy'.
- I am aware that ICT technical staff monitor the use of ICT and the Internet and that if I am found to have been accessing inappropriate material or using ICT inappropriately, this may result in disciplinary action being taken.
- If I have any concerns about any incidents where inappropriate pop-ups or other material inadvertently appears I must email full details immediately to IT technician and report this to the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ONLY use my school email account for all school business and never use my personal email account.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out personal details such as mobile phone numbers and personal email addresses to pupils.
- I will support and promote the school's 'Online Safety and Acceptable Use Policy' and data security.
- I will help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that photographs of children (or staff) will only be taken with school equipment and where the parents' permission has been obtained.
- I will ensure that images of children are not stored on any personal equipment or devices.
- I will ensure that I am complying with the 'Social Networking Policy' (appendix 5 of GBS online policy) and that at no time any images or materials are distributed outside the school without the express permission of the Headteacher.
- Staff laptops and ipads will be subject to random checks to ensure appropriate use.
- All staff have read the Social Networking Sites & Personal Internet Presence for School Staff section of the online safety policy.

Signed: _____ Print Name:_____Date: _____

**Appendix C.** **Acceptable/Responsible Use Agreement for Governors**

GILES BROOK SCHOOL

- I will only use the school's email, Internet, network and any related technologies for professional purposes or for uses defined as 'reasonable' by the Headteacher or governing body.
- I will ensure that personal data (such as data held on SIMs software) is kept secure and is used appropriately on school premises. Personal data can only be taken out of school when authorised by the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out personal details such as mobile phone numbers and personal email addresses to pupils.
- I will support and promote the school's 'Online Safety and Acceptable Use Policy' and data security.
- I will ensure that photographs of children (or staff) will only be taken with school equipment and where the parents' permission has been obtained.
- I will ensure that images of children are not stored on any personal equipment or devices.
- I will ensure that I am complying with the 'Social Networking Policy' and that at no time any images or materials are distributed outside the school without the express permission of the Headteacher.

Signed: _____ Print Name:_____

Date: _____

**Appendix D. Acceptable/Responsible Use Agreement for Parent Helpers/Volunteers/Work Experience Students**

GILES BROOK SCHOOL

- I will only use the school's email, Internet, network and any related technologies for professional purposes or for uses defined as 'reasonable' by the Headteacher or governing body.
- I will ensure that personal data (such as data held on SIMs software) is kept secure and is used appropriately on school premises. Personal data can only be taken out of school when authorised by the Headteacher.
- I am aware that ICT technical staff monitor the use of ICT and the Internet and that if I am found to have been accessing inappropriate material or using ICT inappropriately, this may result in disciplinary action being taken.
- If I have any concerns about any incidents where inappropriate pop-ups or other material inadvertently appears I must log this immediately in the ICT incident log (currently reporting to Jenny in person or via email) and report this to the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not give out personal details such as mobile phone numbers and personal email addresses to pupils.
- I will support and promote the school's 'Online and Acceptable Use Policy' and data security.
- I will help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that photographs of children (or staff) will only be taken with school equipment and where the parents' permission has been obtained.
- I will ensure that images of children are not stored on any personal equipment or devices.
- I will ensure that I am complying with the Social Networking Policy (appendix 5 - GBS online safety policy) and that at no time any images or materials are distributed outside the school without the express permission of the Headteacher.
- Access will be subject to random checks to ensure appropriate use.

Signed: _____ Print Name:_____

Date: _____

**Appendix E.**

**Social Networking Sites & Personal Internet Presence for School Staff**

This policy applies to personal use of social networking sites (for example: Facebook, MySpace, Twitter, Instagram, Tumblr, Pinterest, Whatsapp, Snapchat, Google+, LinkedIn, MSN, Bebo etc), personal web pages, personal space provided by Internet providers and Internet presence including blogs which make available personal views to the general public. This includes web pages or social media pages hosted by Milton Keynes Council which you are visiting as a personal user (not as a moderator). Although LinkedIn is not primarily a social networking site employees should apply the principles set down within this policy to their use of this and similar professional networks.

**Guidance**

- If you already make reference to your employment at the school on a personal internet site as defined above, or you intend to create such a site, you should inform your Headteacher.
- If you do refer to your employment at the school you must use a disclaimer such as "the views contained in these web pages are my personal views and do not represent the views of the School".
- Please be aware that using material from any copyrighted source without permission is likely to breach copyright.
- Carefully avoid bringing the school or its employees into disrepute and consult your Headteacher if you are unsure whether the content is appropriate.
- The school reserves the right to require removal of any material published by an employee which may adversely affect the school's reputation or create risk of legal proceedings against the school.
- Do not reveal information which is confidential to the school - consult your Headteacher if you are unsure.
- Employees must not use social networking sites for party political purposes.
- Do not include or use any school, data, information, contact details or photographs of employees, pupils, parents or partner organisations without the explicit written permission of the school and the explicit written permission of the data subject (e.g. person shown in any photograph).
- Do not include comments or photographs which could bring into question your professional credibility.
- Accessing social networking sites on school premises is not allowed. (This does not include the school Twitter account, which are used for educational purposes.) Time spent accessing social networking sites at work, for personal use, using school equipment must comply with the IT Policy applicable within the school. This includes the use of school equipment at home such as smart phones, tablets or laptops whether during or outside working hours.
- Do not invite or accept as "friends" on such sites: any child or vulnerable adult or the family members of any child or vulnerable adult you have met in the course of your employment.
- If you receive press or media contact regarding the content of your personal site and feel there may be implications for you or which in any way relates to the school, you should consult your Headteacher.

**Managing your personal use of Social Media:**

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life.
- Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

**Managing school social media accounts**

**The Do's**

- Check with a senior leader before publishing content that may have controversial implications for the school
- Do not express personal views on the school social media account
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other people's' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

**The Don'ts**

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

**Compliance**

The School reserves the right to take action under the Disciplinary Policy should employee's breach this policy or bring the school into disrepute by their actions on the Internet. The Disciplinary Policy is available on the Internet at: Disciplinary Policy applicable to Headteachers or Disciplinary Policy applicable to School Staff other than Headteachers

Employees must ensure that their use of social networking sites does not breach the safeguarding guidance as set out in Section 12 of the Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings available on the Department for Education website. Please also consult the "Online safety and Acceptable Use Policy".

**Employee privacy and dignity**

Employees are strongly recommended to check that their online privacy settings only allow "friends" to see their profiles and that the privacy settings of "friends" do not inadvertently allow access to the employee's own profile. It is also advised that as a general measure to protect their personal safety and identity, staff do not accept friend requests from people who are not personally known to them.

Employees may wish to ask friends to check before photographs are posted which may cause them embarrassment. Employees posting their own images should bear in mind the fact that any image can easily be downloaded and manipulated and they should choose which images they share accordingly. It is recommended that employees do not post images that could be used to identify their homes or families.

**Information and training**

All employees are advised to make themselves familiar with the parent/carer or teacher/trainer pages on the CEOP "Think You Know" site at www.thinkyouknow.co.uk A full day's training can also be accessed via www.mkscb.org which incorporates the CEOP internet safety training and information on grooming via the internet. There is no charge for this course.

The MKSCB website also provides links to other online safety information as well as the full inter-agency safeguarding training programme.

**Safety of Young People**

Employees should be aware of the vulnerability of young people online. Employees who use the school blog and email within their work to contact young people should:-

- Always be professional and maintain the highest standards of personal behaviour at all times
- Recognise the trust that is placed in adults by children and treat this trust with the highest respect and responsibility
- Work in an open and accountable manner at all times
- Always use appropriate language and be respectful in any communication
- Not favour or appear to favour any child or show interest in one more than another
- Not discriminate against anyone because of age gender, disability, culture, language, ethnicity, religious beliefs or sexual identity
- Be aware that children may misinterpret your intentions, so ensure that all language is age

*This policy has been compiled using SWGFL Online Safety School / Academy template Policies and Milton Keynes Council Policy on Social Networking Sites & Personal Internet Presence for School Staff 2013. It has also been compiled to support the 'Keeping Children Safe in Education' 2016 document and the Giles Brook Child Protection policy.*