BLANCHE NEVILE SCHOOL
The best of both worlds for deaf children

E-Safety Policy

Author:	Headteacher	Date written:	January 2013
Amended / Reviewed by:	Senior Leadership Team And Safeguarding Committee	Review Date:	November 2019
		Next Review Date:	FGB to decide

Introduction

Computing 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 life-long learning and employment.

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 children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

At Blanche Nevile we understand the responsibility to educate our pupils on eSafety issues. 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 our school to use technology to benefit learners. The school uses the Local Authorities guidance and Judicium for GDPR, in line with national legislation.

A shared responsibility

Everybody in our 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.

Monitoring
Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

Breaches
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.

Data Security
The accessing and appropriate use of school data is something that the school takes very seriously. The school uses the Local Authorities guidance on GDPR, in line with national legislation.

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
- Staff are aware of their responsibilities when accessing school data
- 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, keep it locked out of sight
- 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. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.
- All laptops and iPads to be kept in a secured and locked area when not in use.

Disposal of Redundant ICT Equipment Policy
- Disposal of any ICT equipment will conform to the **Data Protection Act 1998**
- The school's disposal record will include:
- Date item disposed of
- Authorisation for disposal, including:
- Verification of software licensing
- Any personal data likely to be held on the storage media?
- How it was disposed of eg waste, gift, sale
- Name of person & / or organisation who received the disposed item

e-Mail
- The school gives all staff their own e-mail 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 e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. The school email account should be the account that is used for all school business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

e-Mails and Pupils

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil e-mail 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 e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform Management if they receive an offensive e-mail
- However staff access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Receiving e-Mails

- Check e-mail regularly
- Activate 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; Consult the network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

e-mailing Personal, Sensitive, Confidential or Classified Information

- When a member of staff concludes that e-mail must be used to transmit such data:
- Obtain express consent from manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anybody/person whose details have not been separately verified (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt
- Use own school e-mail account so staff member is clearly identified.

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Senior Management and governors are updated by the Headteacher/Deputy Head and all governors 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: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSD.

eSafety in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing and PSD lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils about the online risks that they may encounter outside school is also done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages.
- New staff receive information on the school's 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 eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- eSafety posters will be prominently displayed
- eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to School Management.

Misuse and Infringements

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to Management.

- Deliberate access to inappropriate materials by any user will lead to an investigation by the Headteacher/ LA and could possibly lead to dismissal and involvement of police for very serious offences.

Managing the Internet

- 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. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

Internet Use

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Staff must not reveal names of colleagues, pupils, others or any other confidential information acquired through their role on any social networking site or other online application
- On-line gambling or gaming is not allowed

Infrastucture

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a member of staff
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the (technician/teacher) for a safety check first
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the School Office.

Managing Other Web 2 Technologies

- All pupils are advised to be cautious about the information given by others on social networking websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher

Parental Involvement

- Parents/carers are asked to read through and sign acceptable use agreements 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)
- Parents/carers are expected to sign a Home School agreement containing the following statement or similar
- We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
- Information and celebration evenings
- Practical training sessions e.g. How to adjust the Facebook privacy settings
- Posters
- School website
- Newsletter items

Passwords and Password Security

- Always use passwords that are delegated/given
- Make sure delegated/given passwords are used each time for logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never** tell a child or colleague a password
- If a member of staff is aware of a breach of security with password or account inform the Headteacher/Deputy Head immediately
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and pupils who have left the school are removed from the system immediately.

If staff think a password may have been compromised or someone else has become aware of the password report this to ICT support team

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from own PC or removable media equipment is kept secure
- Staff must ensure that screen is locked before moving away from the computer during the normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Only download personal data from systems if expressly authorised to do so by manager

- Staff must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Staff to keep screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data

Please refer to the document on the grid for guidance on How to Encrypt Files

- http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Remote Access

- Staff are responsible for all activity via remote access facility
- Only use equipment with an appropriate level of security for remote access
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Safe Use of Images

Taking of Images and Film

- 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 are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others.
- Pupils and staff must have permission from the Headteacher/Deputy Head before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought and a copy is located in the personnel file

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 web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes

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, eg divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.

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

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the School Marketing and Communication Officer, Primary Admin Assistant or the Headteacher has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network

CCTV

- The school uses CCTV for security and safety. The only people with access to this are School Management and designated Office staff. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

- As a user of the school ICT equipment, staff are responsible for their own activity
- **Visitors are not allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available**
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- Staff must 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
- On termination of employment, resignation or transfer, return all ICT equipment to Manager. Staff must also provide details of all system logons so that they can be disabled
- It is staff's responsibility to ensure that any information accessed from own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

Portable & Mobile ICT Equipment

- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by our ICT support

Personal Mobile Devices (including phones)

- Pupils may be allowed to bring personal mobile devices/phones to school but must not use them within lesson time or in the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed and in line with the school's Behaviour Policy dated January 2018, may result in a C4 exclusion
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed

LGFL eSafety guidelines to be displayed throughout the school

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Twitter to communicate with parents and carers. The Headteacher is responsible for all postings on these technologies and on Facebook monitors responses from others
- **Staff are advised not to access their personal social media accounts at any time during school hours on school equipment.**
- Pupils are not permitted to access their social media accounts on school equipment whilst at school
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law
- Staff are not permitted to name have access or an account with pupils in social media

Systems and Access

- Staff are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC
- Use only delegated/given logons, account IDs and passwords and do not allow them to be used by anyone else
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act. The school uses the Local Authorities guidance on GDPR, in line with national legislation.

Telephone Services

- School telephones are provided specifically for school business purposes.

Mobile Phones

- Report the loss or theft of any school mobile phone equipment immediately
- School SIM cards must only be used in school provided mobile phones
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

AM

Appendix 1

Summary

Review Procedure

There will be on-going opportunities for staff to discuss with Management.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

Further help and support

Freedom of Information Act 2000: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

Advice on esafety - http://www.thegrid.org.uk/eservices/safety/policies.shtml

Test our online safety skills [http://www.getsafeonline.org]

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for our own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Appendix 2

Primary Pupil Acceptable Use – (Guidelines)

Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail 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 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 contacted if a member of school staff is concerned about my eSafety.

Appendix 3 (To be sent with Primary Pupil Acceptable Use Guidelines-Agreement e-Safety Rules)

Dear Parent/ Carer

E-Safety at Blanche Nevile School

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with our child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Veronica Held, Headteacher.

Many thanks for your support.

Kind regards

Geraldine Santiago
Headteacher

Pupil and Parent/Carer signature.....

We have discussed this document and .....(pupil name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at Blanche Nevile School.

Parent/ Carer Signature .....

Class..... Date .....

Appendix 4

Secondary Pupil Acceptable Use – (Guidelines)

Agreement / eSafety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Headteacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- 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 will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.
- I will only use my own personal external storage device but not mobile phone in school. I understand that, if I do use my own external storage device in Blanche Nevile School, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

Appendix 5 (To be sent with Secondary Pupil Acceptable Use Guidelines-Agreement e-Safety Rules)

Dear Parents and Carers

e-Safety at Blanche Nevile School

I am writing to ask for our support in ensuring that students are aware of how to stay safe when using the internet. At school we teach our students how to stay safe on-line and how to behave appropriately on-line. In order to develop a home-school partnership on on-line safety, I would like you to discuss the attached 'Acceptable Use Agreement' and sign it with our child. If you have any concerns or queries, please do not hesitate to get in touch.

Please fill in and return the bottom section of this form by:

Many thanks once again

Kind regards

Geraldine Santiago
Headteacher

Pupil and Parent/Carer signature.....

We have discussed this document and .....(student name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at Blanche Nevile School.

Parent/ Carer Signature .....

Pupil Signature.....

Form ..... Date .....

Appendix 6

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- 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 my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of Blanche Nevile School.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature ..... Date .....

Full Name .....(printed)

Job title .....

Appendix 7

Blanche Nevile School Staff E-mail disclaimer

The wording below will be attached to all emails sent from Blanche Nevile School

Please consider the environment. Do you really need to print this e-mail?

> This email and any files transmitted with it may contain confidential and/or privileged information. It is intended solely for the people or organisations to whom it is addressed. If you are not the intended recipient, any unauthorised copying, disclosure, distribution or other action relating to it is forbidden.
>
> This e-mail does not constitute a legally binding agreement. Views or opinions presented in this email do not necessarily represent those of Blanche Nevile School.
>
> We have taken precautions to minimise the risk of transmitting software viruses, but advise you to do our own virus checks. We cannot accept liability for any loss or damage caused by software viruses.