Griffin Primary School

Online Safety Policy

2016

VENN

CONTENTS

Guidance

This policy has been developed by the SLT, after consultation with Primary Technologies, the IT provider. It is intended for staff and pupil use, and will be ratified by the governing body prior to distribution.

The Acceptable Use Agreement should be issued to the appropriate user for signature and collated by a designated member of staff.

The school should ensure that all persons, including Governors and pupils, who join the establishment mid-year are provided with the policy and agreement.

Vision and Rationale

At Griffin Primary School, we believe that computing offers children the opportunity to develop ways of thinking and understanding that empowers them in an ever changing world. We are committed to enabling all pupils, regardless of background or ability, to achieve their full potential and to be equipped with the skills needed to be successful in their education and beyond. We recognise that children will have different starting points and different home access to technology but believe that this should not be a barrier to their success. We will offer children a broad and balanced curriculum which develops their use and understanding of computer-based technology, as well as using technology as a tool for learning. We will make use of technology to support children of different abilities wherever necessary. We encourage all members of the school community to develop positive attitudes towards computing. We aim to ensure that all users know how to stay safe when using digital devices and we put E-safety at the heart of everything we do. We will offer children a range of digital devices, areas of study and opportunities to put their learning into context.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement

- Illegal downloading of music or video files

- The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents/carers and the wider community) to be aware and to assist in this process.

Monitoring and Security

Authorised IT support staff may inspect any Computing equipment owned or leased by the School at any time without prior notice.

IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School Computing; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by Computing authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA), the Lawful Business Practice Regulations 2000 and Sensitive Data

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised staff.

Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for Computing Acceptable Use

- Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile Computing equipment or removable storage media in unattended vehicles. Where this is not possible, it should be kept locked out of sight.

- It is the legal responsibility of individual staff to ensure the security of any sensitive, confidential and classified information contained in documents copied, scanned or printed. Such devices should not be used for personal data or information. This is particularly important when shared devices are used.

- All staff must sign our mobile devices / ICT equipment user agreement.

- On the occasion that ICT equipment needs to be taken off site, it must be booked out by the school office.

- If a staff member takes any ICT equipment off site they are responsible for the safety and security of the equipment. Any loss or damage could result in a financial penalty e.g. if an item is stolen, we expect staff to inform Police at the earliest opportunity to obtain a crime number and report the missing item to Headteacher. If any item is damaged please inform the Headteacher.

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 or, where appropriate, the local authority Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

Conduct assessments to check organisations are complying with the Act;

Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;

Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

Prosecute those who commit criminal offences under the Act;

Conduct audits to assess whether organisations processing of personal data follows good practice,

Report to Parliament on data protection issues of concern

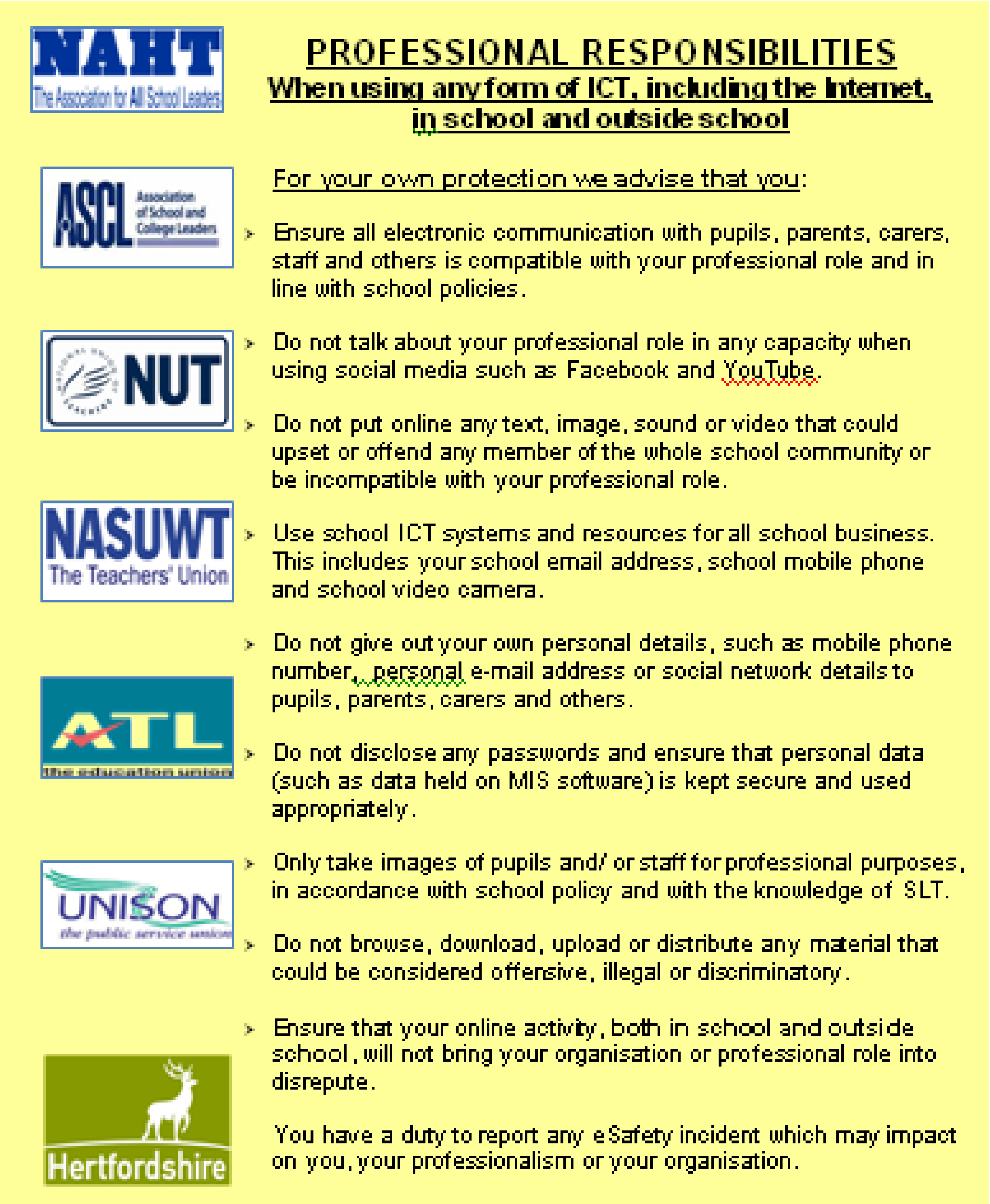
Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the headteacher

Please refer to the section Incident Reporting, Online Safety Incident Log & Infringements.

Staff Professional Responsibilities

These are a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions.



PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used
- Never interfere with any anti-virus software installed on school ICT 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 team
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Online Safety Lead, who will advise you what actions to take and be responsible for advising others that need to know

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette' and this is covered in the curriculum.

Managing e-Mail

- The school gives relevant 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. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- All e-mails should be written carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000
- Staff must inform the Headteacher if they receive an offensive e-mail

Sending e-Mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Never open attachments from an untrusted source
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has less than age appropriate 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.

Online Safety

Online Safety - 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 named online Safety lead in this school is the Headteacher who has been designated Online Safety Lead. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Lead to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Online Safety Lead 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, whistle-blower, equality, PSHE and Code of Conduct.

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.

The school has a framework for teaching internet skills in Computing lessons

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

Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

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 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 Computing curriculum

Online Safety Skills Development for Staff

Our staff receive regular information and training on Online Safety 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 Online Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)

All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas

Managing the School Online Safety Messages

We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used

The Pupil Acceptable Use Policy will be introduced to the pupils at the start of each school year

Online Safety posters will be prominently displayed

Incident Reporting, Online Safety 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. Additionally, all security breaches, lost/stolen equipment or data), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the headteacher.

Misuse and Infringements

Complaints
Complaints and/ or issues relating to Online Safety should be made to the Headteacher. Incidents should be logged

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged, depending on the seriousness of the offence; investigation by the Headteacher

Internet Access

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.

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 could be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/carers 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

Smoothwall/Primary Technologies provide filtering for all users

Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

On-line gambling or gaming is not allowed

Personal on-line shopping of any type is not allowed

It is at the Headteacher’s discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

Our school also employs some additional web-filtering which is the responsibility of Primary Technologies

Griffin Primary school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

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

If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Online Safety Lead or teacher as appropriate

It is the responsibility of the school, by delegation to the network manager/Primary Technologies, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT subject leader.

If there are any issues related to viruses or anti-virus software, the network manager should be informed

Managing Other Web 2.0 Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavors to deny access to social networking and none-educational online games websites to pupils within school

All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) 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, IM/ 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

Pupils are asked to adhere to age recommendations on social media sites

Our pupils are asked to report any incidents of Cyberbullying to the school

Parental Involvement

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.

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 stating their support

The school disseminates information to parents/carers relating to Online Safety where appropriate in the form of;

- Information and celebration evenings
- Training sessions
- Posters
- School website
- Newsletter items

Passwords and Password Security

Passwords

Always use your own personal passwords

Make sure you enter your personal passwords each time you 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 your 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 your password

If you are aware of a breach of security with your password or account inform the Online Safety Lead immediately

Passwords must contain a minimum of six characters and be difficult to guess.

Passwords should contain a mixture of upper and lowercase letters, numbers and symbols

User ID and passwords for staff and pupils who have left the school are removed from the system

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

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others

Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and MIS systems including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Zombie Accounts

Zombie accounts refers 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.

Ensure that all user accounts are disabled once the member of the school has left

Prompt action on disabling accounts will prevent unauthorized access

Safe Use of Images

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/carers (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

Staff and 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

Pupils and staff must have permission from the Headteacher 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 on induction 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

recorded/ transmitted on a video or webcam

in display material that may be used in the school's communal areas

in display material that may be used in external areas, ie exhibition promoting the school

general media appearances, eg 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, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents/carers in order for it to be deemed valid.

Pupils' 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.

Storage of Images

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

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

Video Conferencing

Permission is sought from parents/carers if their children are involved in video conferences

Permission is sought from parents/carers if their children are involved in video conferences with end-points outside of the school

All pupils are supervised by a member of staff when video conferencing

All pupils are supervised by a member of staff when video conferencing with end-points beyond the school

No part of any video conference is recorded in any medium without the written consent of those taking part

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

School ICT Equipment

It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

Do not allow your visitors 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

Ensure that all ICT equipment that you use is kept physically secure

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

It is imperative that you save your data on a frequent basis to the school network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.

Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick, or other portable device. If it is necessary to do so the local drive must be encrypted

On termination of employment, resignation or transfer, return all ICT equipment to the School Business Manager. You must also provide details of all your system logons so that they can be disabled

It is your responsibility to ensure that any information accessed from your 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

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

All activities carried out on school systems and hardware will be monitored in accordance with the general policy

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. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

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 your ICT support

In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, tablets/iPads and games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones) *– refer to the code of conduct policy*

The school allows staff to bring in personal mobile phones and devices for their own personal use only. Under no circumstances does the school allow a member of staff to contact a parent/carers or pupil using their own personal device/s or use their own device to take images of staff or pupils. Mobile phones must be switched off during the working day, unless in the case of emergency, in which case the Headteacher should be informed.

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

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

---

Removable Media

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the ICT team

Social Media

- Our school uses Parent Mail, Marvellous Me and Twitter to communicate with Parents/Carers. Specific named staff are responsible for all postings on these technologies.
- Staff, governors, pupils, parents/carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents/carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- 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 access their own social media accounts whilst on school premises
- Staff should use personal social media accounts in a responsible and professional manner to ensure they don't put themselves or the school at risk
- Staff should not include parents/carers on their personal social contacts, This is deemed to be inappropriate as these can be misconstrued as official communication channels between school and wider community

Writing and Reviewing this Policy

Review Procedure

There will be on-going opportunities for staff to discuss with the Headteacher any Online Safety issue that concerns them

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

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been read, amended and approved by the staff, head teacher and governors on 11th July 2016

Reviewed by

This policy should be read in conjunction with the following School Policies

- Code of Conduct Policy
- Child Protection Policy
- Behaviour Policy
- Prevent Policy

Current Legislation

Acts Relating to Monitoring of Staff eMail

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

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

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

Other Acts Relating to Online Safety

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 your 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.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

access to computer files or software without permission (for example using another persons password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud) impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

REFERENCES

Particularly for Parents

National Action for Children (NCH)
Parents Guide on Internet usage www.nchafc.org.uk/itok/itokhome.html
Current activities to promote safe use www.nchafc.org.uk/internet

Internet Watch Foundation - report inappropriate Web sites www.iwf.org.uk
Safe Surfing Guide for parents and carers: www.internetwatch.org.uk/safe/index.htm
Which article on Internet filtering for home use
www.internetwatch.org.uk/safe/which/total.htm

Parents Information Network (PIN) www.pin.org.uk
Comprehensive guidelines on Internet safety

Recreational Software Advisory Council (RSACi) www.rsac.org/
Promotes rating systems for Web sites, and is a third party rating bureau

Particularly for Schools

Associations of Co-ordinators of IT (ACITT)
http://atschool.eduweb.co.uk/acitt/aup.html
Acceptable use policy for the Internet in UK Schools

BECTa www.becta.org.uk/technology/infosheets/html/accuse.html
Advice and guidance on appropriate computer use

British Computer Society www.bcs.org.uk/iap.html
A guide for schools prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

DfES Superhighway Safety http://safety.ngfl.gov.uk
Essential reading. For free pack telephone: 0845 6022260

Internet Watch Foundation - www.iwf.org.uk
Invites users to report illegal Web sites

Kent NGfL Initiative www.kented.org.uk/ngfl/

Curriculum material for schools including this Internet Policy

Kent Web Skills Project www.kented.org.uk/ngfl/webskills/
A Web site which discusses the research process and how the Web is best used in projects.

Scottish Education Department www.scotland.gov.uk/clickthinking
Comprehensive safety advice

SEGfL ICT Security Policy www.segfl.org.uk/
An overview of the security of networks with Internet access.

Copyright www.templetons.com/brad/copymyths.html
Covers the main aspects of copyright of digital materials, US-based but relevant.

Internet Users Guide www.terena.nl\libr\gnrt\
A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web

Acceptable Use Agreement: Pupils

This will be signed by children at the beginning of each year

Primary Pupil Acceptable Use Agreement / Online Safety Rules

I will only use Computing equipment in school for school work.

Mobile phones must not be used in school.

I will take care of the Computing devices and treat them with respect.

I will make sure that all Computing contact with other children and adults is responsible, polite and sensible.

I will not give out my personal details.

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 or wider community.

If I encounter an unacceptable image on a computer screen, I will report it immediately to my teacher.

I know that my use of Computing technologies can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Safety.

Pupil User Signature

I agree to follow this code of conduct and to support the safe and secure use of Computing throughout the school. I understand that if I do not follow this code of conduct it may result in the temporary or permanent withdrawal of school Computing hardware, software or services.

Signature ……………………………………………………………………………. Date ……………………

Full Name ………………………………………………………………………………(printed) Class . . . .

Dear Parent/ Carer

Computing, including the use of the internet, e-mail and mobile technologies etc, is an important part of learning in our school. We expect all children to be safe and responsible when using any Computing equipment.

Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school.

✂

Parent/ carer signature
We have discussed this and ……………………………………......(child name) agrees to follow the Online Safety rules and to support the safe use of Computing Griffin Primary School.

- 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 them into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the school's 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.

Parent/ Carer Signature …………………………………………………….

Pupil Signature …………………………………………………………………….

Class ………………………………… Date ……………………………………….

Acceptable Use Agreement: Staff, Governors, Student teachers and Visitors

Computing (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 Computing equipment. 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 SLT or 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 Computing 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 personal e-mail address, social media account details to parents/carers or pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data 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 the Online Safety Lead.
- 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 using school ICT equipment only 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 support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my personal online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's Online Safety policies and Data Security policies and help pupils to be safe and responsible in their use of Computing and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

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

Signature ……………………………………………………………………… Date ……………………

Full Name ……………………………………..(printed)

Job title ……………………………………………………………………….

iPad User Agreement and Acceptable Use Policy – Teachers

iPads allocated to teachers are the property of Griffin Primary School and should be looked after with appropriate care. Teacher use of the iPad falls under the School's Acceptable Use of ICT Policy for Staff, its Child Protection Policy, Online Safety Policy and Code of Conduct. In Griffin Primary school, access to the internet will be monitored through the school's content filtering service and the device will be monitored and by Mrs L Bell, School Business Manager.

Provision of Equipment

Staff will be given an iPad mini, protective case and charger.

Staff should:

- remember that iPads must be used for educational purposes only;
- follow the School's Acceptable Use of ICT Policy for staff the Child Protection Policy and Code of Conduct Policy at all times;
- keep their iPad with them or in a secured (locked) area in school at all times. You must not take the ipad home it is school property and must be locked away each day.
- keep the four digit security PIN on their iPads confidential;
- report loss, theft or damage to Headteacher immediately;
- back up data securely by ensuring iCloud is enabled at all times.
- Ensure that any member of staff borrowing their iPad, is fully aware of the iPad AUP

Staff should not:

- modify the settings of their iPads in any way unless instructed by Mrs L Bell
- apply any permanent marks, decorations or modifications to their iPads;
- remove their iPads from their protective cases.
- Link personal devices or iClouds to the school iPad.

Using the IPAD

- Primary Technologies will initially set up the iPad and these settings should not be changed by staff.
- Clean the screen often with approved cleaning towels and keep away from food and drink.
- Charge the iPad only with an Apple charger and standard wall outlet for your powersource.
- Any errors or problems with the iPad should be reported to Mrs L Bell as soon as possible.

Apps

- Apps for use in school should be purchased/installed through Mrs L Bell
- Key apps will be pre-installed on each iPad.

Staff iPad User Agreement

I agree to use the iPad allocated to me for educational purposes, including with pupils in teaching spaces in Griffin Primary School. I understand and will abide by the use of iPad regulations outlined above, in conjunction with the School's Acceptable Use of ICT Policy and the Child Protection Policy. I further understand that should I commit any violation the School may ask me to return the iPad and school disciplinary or legal action may ensue. I also agree to periodically hand in my iPad for routine maintenance, security up-dating and screening. In the case of a suspected theft, I will ensure that a Police Report is completed in liaison with the Headteacher and an Incident Number provided to the School.

User's Full Name:

User's Signature:

Date:

iPad User Agreement and Acceptable Use Policy – SLT

iPads allocated to SLT are the property of Griffin Primary School and should be looked after with appropriate care. Teacher use of the iPad falls under the School's Acceptable Use of ICT Policy for Staff, its Child Protection Policy, Online Safety Policy and Code of Conduct. In Griffin Primary school, access to the internet will be monitored through the school's content filtering service and the device will be monitored and by Mrs L Bell, School Business Manager.

Provision of Equipment

Staff will be given an iPad, protective case and charger.

Staff should:

- remember that iPads must be used for educational purposes only;
- follow the School's Acceptable Use of ICT Policy for staff the Child Protection Policy and Code of Conduct Policy at all times;
- keep their iPad with them or in a secured (locked) area in school at all times.
- keep the four digit security PIN on their iPads confidential;
- report loss, theft or damage to Headteacher immediately;
- back up data securely by ensuring iCloud is enabled at all times.
- Ensure that any member of staff borrowing their iPad, is fully aware of the iPad AUP

Staff should not:

- modify the settings of their iPads in any way unless instructed by Mrs L Bell
- apply any permanent marks, decorations or modifications to their iPads;
- remove their iPads from their protective cases.
- Link personal devices or iClouds to the school iPad.

Using the IPAD

- Primary Technologies will initially set up the iPad and these settings should not be changed by staff.
- Clean the screen often with approved cleaning towels and keep away from food and drink.
- Charge the iPad only with an Apple charger and standard wall outlet for your powersource.
- Any errors or problems with the iPad should be reported to Mrs L Bell as soon as possible.

Apps

- Apps for use in school should be purchased/installed through Mrs L Bell
- Key apps will be pre-installed on each iPad.

Staff iPad User Agreement

I agree to use the iPad allocated to me for educational purposes, including with pupils in teaching spaces in Griffin Primary School. I understand and will abide by the use of iPad regulations outlined above, in conjunction with the School's Acceptable Use of ICT Policy and the Child Protection Policy. I further understand that should I
commit any violation the School may ask me to return the iPad and school disciplinary or legal action may ensue. I also agree to periodically hand in my iPad for routine maintenance, security up-dating and screening. In the case of a suspected theft, I will ensure that a Police Report is completed in liaison with the Headteacher and an Incident Number provided to the School.

User's Full Name:

User's Signature:

Date: