2016

# On-Line Safety and Acceptable Use of IT Policy

# September 2016

**Contents**



**Appendices**

2016



## 1 Introduction

IT 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 Communications 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 IT 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, forums, chat rooms and chat apps such as WhatsApp, Kik and Snapchat
- Photo sharing apps and websites including Instagram and Flickr
- Video chat apps and websites including Skype, Hangouts, Face Time, Chatroulette and Omegle
- 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
- Vlogs, Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

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

At Priory Rise, we understand the responsibility to educate our pupils on On-Line Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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

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

## 2 Roles and Responsibilities

As On-Line Safety 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. The IT leader is the On-Line Safety co-ordinator who has been designated this role to advise and inform the senior leadership team. All members of the school community have been made aware of who holds this post.

The senior leadership team and governors are updated by the Headteacher and 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, Behaviour (including the anti-bullying) and PSHE.

## 3 On-Line Safety in the Curriculum

IT and on-line resources are increasingly used across the curriculum. We believe it is essential for On-Line Safety guidance to be given to the pupils on a regular and meaningful basis. On-Line Safety is embedded within our curriculum and we continually look for new opportunities to promote On-Line Safety.

- The school provides opportunities within a range of curriculum areas to teach about On-Line Safety.

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the On-Line Safety curriculum.

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- Pupils are taught about copyright, respecting other people's information and protecting their own personal information, safe use of images and other important areas through discussion, 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.

- Educating pupils about the dangers of "sexting" (the making and distribution of self-taken images featuring nudity or explicit content) as part of the On-Line Safety curriculum.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the IT curriculum.

## 4 Pupils with Additional Needs

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

## 5 E-Mail

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private.

- 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. 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.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

- E-mails created or received as part of staff roles will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage e-mail accounts as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- The forwarding of chain letters is not permitted in school.

- All 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. Emails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, emails should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.

- Staff must inform (the On-Line Safety co-coordinator or Headteacher) if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

**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.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

- School e-mail is not to be used for personal advertising.

**Receiving E-Mails**

- Check your e-mail regularly.

- Activate your 'out-of-office' notification when away for extended periods.

- Never open attachments from an untrusted source; Consult the IT leader or technician first if in doubt.

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

- The automatic forwarding and deletion of e-mails is not allowed.

## 6 On-Line Safety Support for Staff

- Our staff receive regular and appropriate information and training on On-Line Safety and how they can promote the 'Stay Safe' online messages. This is usually through the usual scheduled programme of staff meeting.

- 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 On-Line Safety 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 On-Line Safety activities and awareness within their curriculum areas.

## 7 The Internet

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- 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.
- 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.
- On-line gambling or gaming is not allowed.
- All staff, volunteers and governors must comply with the Social Networking Policy regarding the posting of any information or images relating to the school.
- School internet access is controlled through the E2BN web filtering service.
- Priory Rise is aware of its responsibility when monitoring staff communication under current legislation.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the On-Line Safety coordinator or teacher as appropriate.
- It is the responsibility of the school, 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 IT leader.
- If there are any issues related to viruses or anti-virus software, the IT leader should be informed.

- The school does not allow any access to social networking sites.

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

## 8 Taking of Images and Film

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

- Staff and visitors are not permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. Appropriate images can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted from the individual device.

- 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.

- Staff must have permission from the Headteacher before any image can be uploaded for publication.

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

- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.

## 9 Publishing Pupil's Images and Work

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

- on the school 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, i.e. exhibition promoting the school.

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

2016

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

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 a child's work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

## 10 Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restrITed to the teaching staff and pupils within the confines of the school network or other online school resource.

## 11 Web Cams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Staff must ensure web cams are switched off when not in use.

## 12 Video Conferencing

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

## 13 Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Staff should not use personal mobile devices to contact a pupil or parent/carer unless in exceptional circumstances and with the prior approval of the Headteacher.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate messages, images (including pseudo images), videos or sounds between any members of the school community is not allowed.

- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.

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

## 14 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).

- The school disseminates information to parents relating to On-Line Safety where appropriate in the form of:

    - Information and celebration evenings
    - Practical training sessions
    - Newsletter items

## 15 Security

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

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others.

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for IT Acceptable Use

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

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

- Staff should always carry portable and mobile IT equipment or removable media as hand luggage, and keep it under your control at all times

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

- All IT equipment is security marked as soon as possible after it is received. The

bursar maintains a register of all IT equipment and other portable assets.

- As a user of the school IT equipment, you are responsible for your activity.
- IT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory.
- It is imperative that staff save your data on a frequent basis to the school's network. Staff 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 devices. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned IT equipment should not be used on a school network unless in exceptional circumstances and with the prior approval of the Headteacher. In these cases devices should be connected to the "guest" WiFi network only.
- On termination of employment, resignation or transfer, staff must return all IT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- 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.
- The installation of any applications or software packages must be authorised by the IT leader.
- Portable equipment must be transported in its protective bag.
- Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

**Server Security**

- School servers are kept in a locked and secure environment and there are limited access rights to these which are password protected.
- Existing servers should have security software installed appropriate to the machine's specification and the school uses a remote back up service and data is backed up daily.

**Using Removable Media**

- Always consider if an alternative solution already exists.

- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by your IT support team.

**Monitoring**

- Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices.

- Internet activity is logged by the school's internet provider and in addition the school's technician regularly monitors the web sites which are accessed on school equipment.

## 16 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 IT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

## 17 Incident Reporting

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

An incident log is used to monitor what is happening and identify trends or specific concerns. The log is kept in the school office.

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

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the On-Line Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, possibly leading to disciplinary action, dismissal and involvement of police for very serious offences.

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

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access

- Personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- The security of any personal, sensitive, confidential and classified information contained in documents which are faxed, copied, scanned or printed.

- Only download personal data from systems if expressly authorised to do so by the Headteacher.

- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

- Hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

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

**19 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 IT equipment that you use.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact your IT support provider immediately. The IT support provider will advise you what actions to take and be responsible for advising others that need to know.

**20 Disposal of IT Equipment**

- All redundant IT equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant IT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- All redundant IT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

Disposal of any IT equipment will conform to current legislation and will confirm with the governors' policy on the disposal of equipment.

**21 Zombie Accounts**

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

- Technical staff will ensure that all user accounts are disabled once the member of the

school has left the school.

## Acceptable/Responsible Use Agreement and Safety Rules for Pupils

- I will only use IT in school for school purposes.
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will make sure that all IT 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 IT because I know that these rules are to keep me safe.
- I will not send photographs or videos or any other information about myself to others.
- I will support the school approach to onlinOn-Line 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 IT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

**Pupil's Agreement**

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

Signed: _____ Class: _____

Date: _____

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

I have read and understood the school rules for responsible computer and internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Please Print Name: _____

Date: _____

# Acceptable/Responsible Use Agreement for Staff

- I will only use the school's email, internet, network and any related technologies for professional purposes or for uses defined as 'reasonable' by the Headteacher or governing body.

- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately on school premises. Personal data can only be taken out of school when authorised by the Headteacher.

- I will only use a school memory stick and not my own personal devices for storing information. (Memory sticks are available from the IT leader.)

- I will not install any hardware or software without permission of the Headteacher or IT leaders.

- I am aware that I may use my school laptop for personal use, however I must ensure that at no time this is being used inappropriately or inappropriate material is being accesses – this includes any materials that could be considered offensive, illegal or discriminatory. I will ensure that my use of IT is in keeping with the On-Line Safety Policy.

- I am aware that IT technical staff monitor the use of IT and the internet and that if I am found to have accessing inappropriate material or using IT inappropriately this may result in disciplinary action being taken.

- If I have any concerns about any incidents where inappropriate pop-ups or other material inadvertently appears I must log this immediately in the IT incident log and report this to the Headteacher.

- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out personal details such as mobile phone numbers and personal email addresses to pupils.

- I will support and promote the school's On-Line Safety Policy and data security and help pupils to be safe and responsible in their use of IT and related technologies.

- I will ensure that photographs of children (or staff) will only be taken with school equipment and where the parents' permission has been obtained.

- I will ensure that images of children are not stored on any personal equipment or devices.

- I will ensure that I am complying with the Social Networking Policy and that at no time any images or materials are posted or distributed outside the school without the express permission of the Headteacher.

Signed: _____ Date: _____