DOWSON PRIMARY SCHOOL

E Safety Policy

2015

E-Safety Policy

Dowson Primary School e-Safety Policy

Contents of e-Safety Policy:

8. Data Protection policy

9. ICT Loans to staff – agreement form

Appendix A - Using Social Media Responsibly

Appendix B - Laptop Users Policy

Appendix C - ICT Acceptable Usage Policy (staff)

Appendix D - ICT Security Policy

Appendix E - Google Apps Permision

Appendix F - ICT Acceptable Usage Policy (pupils)

1. Introduction

Our e-Safety Policy has been written by the school.

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

To be revised: October 2016

2. Context and Background

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

• An effective range of technological tools;

• Policies and procedures, with clear roles and responsibilities

• E-Safety teaching is embedded into the school curriculum and schemes of work

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

Leadership team

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures

Governors

The School Governing body is responsible for overseeing and reviewing all school policies,

including the e-Safety Policy.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed.

They should sign the Staff Acceptable Internet Use agreement annually

Class teachers should ensure that pupils are aware of the e-Safety rules, introducing them at the beginning of each new school year and lessons as in the E-Safety section of the curriculum.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school. (Appendix F)

Parents

Parents are given information about the school's e-safety policy on the website. They are given copies of the pupils acceptable usage agreement, and asked to support these rules with their children.

4. Technical and hardware guidance

School Internet provision

The school use a standard secure Internet Service Provider.

Content filter

Dowson Primary School use a Fortigate content filter to ensure that as far as possible, only appropriate content from the Internet finds it way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

• All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.

• Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

• Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

Portable storage media

• Staff are allowed to use their own portable media storage (USB Keys etc). If use of such a device results in an anti-virus message

they should remove the device and immediately report to the System Manager.

Security and virus protection

The school subscribes to AVG Antivirus software program. All software is monitored and updated regularly by the school technical support staff.

• Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the System Manager immediately.

5. E-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

a.Internet access at school

Use of the Internet by pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

Out of Hours Provision

There is an after-school club that runs each day after school. There will be no unsupervised access to the Internet at any time during Out of Hours provision.

b.Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum (Sept 2014)

We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand

who has made this information available, and how accurate and truthful it is.

• Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.

• Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.

• They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.

• They are taught how to carry out simple checks for bias and misinformation

• They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

c.Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home.

The main aspects of our approach include the following five SMART tips:

Safe - Staying safe involves being careful and not giving out your name, address, mobile phone number, school name or password to people online...

Meeting someone you meet in cyberspace can be dangerous. Only do so with your

parents'/carers' permission and then when they are present...

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...

Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Were possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. We also feel it is invaluable to teach children how to stay safe when using social media sites at home.

As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.

There is a selection of links to such resources available from on the school website, on the year group blogs and in the web link folder on the children's desktop.

Unsuitable material

Despite the best efforts of the school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Making a note of the website and any other websites linked to it.

2. Informing the System Manager.

3. Discussion with the pupil about the incident, and how to avoid similar experiences in future

d.Using E-Mail at school

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

• We teach the use of e-mail as part of our ICT curriculum in Years 3,4,5 and 6, and use appropriate pupil email accounts where necessary

• Pupils are not allowed to access personal e-mail using school Internet facilities Chat, discussion and social networking sites.

• Pupils and their parents should sign a google permission letter before children are allowed to access the programme. (Appendix E)

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

Internet policy

Pupils may take part in discussion forums or post messages on blogs that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

f.Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

• Pupils are not allowed to have personal mobile phones or other similar devices in school during school hours.

Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

g. Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

• No access to public chat-rooms, Instant Messaging services and bulletin boards.

• Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

• Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

• Complaints related to child protection are dealt with in accordance with school child protection procedures.

h. Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous

School and pupil websites – pictures and pupil input

As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create blog posts. These posts will be checked be class teachers before they are published on the web.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted.

Permission will sought from parents before any child's picture is published on the internet.

i. Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should displayed in each classroom and the ICT suite

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

Initial warning from class teacher

Report to Headteacher

Letter to parent/carer

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc)

Incident logged and reported to Head teacher

Initial letter to parent/carer

Removal of Internet privileges/username etc

Meeting with Parent/Carer to re-sign Internet use agreement

Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

j. How will complaints regarding e-Safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee

that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

• All incidents will be recorded

• Interview/counselling by class teacher, Senior Management Team, e-Safety Coordinator

and Headteacher;

• informing parents or carers;

• removal of Internet or computer access for a period,

• referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

k. Class Rules for responsible ICT use

Keep safe: Keep SMART

1. I will ask permission before using any ICT equipment (e.g. computers, digital cameras, etc), and only use it when a teacher or another adult is with me.

2. I will only use the school's computers for schoolwork and homework.

3. I will only delete my own files, and I will not look at other people's files without their permission.

4. I will use the usernames and passwords provided by the school to access the school network

5. I will not bring software or USB memory sticks into school without permission

6. I will ask permission before using the Internet, and only use it when a staff member is present

7. I will only visit web sites that I am asked to by school staff, or that have been saved in a shared internet link folder for pupils to use

8. I will not use Google image search without being asked to do so by a school staff member.

9. I will not download anything (files, images etc) from the Internet unless given permission

10. I will only use an approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts (e.g. Hotmail) at school.

11. The messages I send or information I upload as part of my school work will always be polite.

12. I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission

13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell a school staff member

14. I understand that the school may check my computer files, e-mail and the Internet sites I visit, to help keep me safe.

15. I understand that if I deliberately break these rules my parents and the Headteacher will be informed.

9. Use of the Internet and ICT resources by school staff

The Internet

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use.

ICT Equipment and Resources

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software

Professional use

Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with

appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support in using ICT as part of their professional practice can ask for support from the ICT Co-ordinator.

Personal use of the Internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the System Manager and Headteacher. The appropriate forms and agreements must be signed.

However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the Laptop Users Agreement detailed below in this document.(appendix B)

E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in the Using Social Media Responsibly Policy – Details in this policy. (Appendix A)

Data Protection and Copyright

The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary. Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

E-Safety Policy Staff Agreement Form (Based on ICT Acceptable Usage policy, Appendix C)

This document covers use of school digital technologies, networks etc both in school and out of school.

Access

• I will obtain the appropriate log on details and passwords from the System Manager.

• I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.

• If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

• I will not allow unauthorised individuals to access school ICT systems or resources

Appropriate Use

• I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

• I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.

• I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network

• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the eSafety coordinator or member of the SMT.

Professional Conduct

• I will not engage in any online activity that may compromise my professional responsibilities

• I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are

not confused with my professional role

• I will never include pupils or former pupils as part of a non-professional social network or group

• I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities

• I will not browse, download or send material that could be considered offensive to colleagues

• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.

Personal Use

• I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.

• I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.

• I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.

Email

• I will only use the approved, secure email system for any school business: (currently: Google For Education Mail)

• I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

• I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.

• I will return school equipment regularly (to be agreed with System Manager) to be checked and updated.

• I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software. Unless checked and authorised by the IT Manager.

Teaching and Learning

• I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet.

• I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials.

• I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.

• I will only use the Internet for professional purposes when pupils are present in an ICT suite, or a classroom with Internet access.

Photographs and Video

• I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.

• I will never associate full pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

Data protection

• I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.

• I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media

• I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises.

• I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission.

• I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Copyright

• I will not publish or distribute work that is protected by copyright

• I will encourage pupils to reference online resources and websites when they use them in a report or publication

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the

school's most recent e-safety policies.

I agree to have a school user account, be connected to the Internet via the school network and be able

to use the school's ICT resources and systems.

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

Full Name ..... (printed)

Job title

.....

School

.....

Appendix A

Using Social Media Responsibly Policy

Policy Issue Record

TMBC

Issue 1 Feb 2012

Issue 2 May 2015

Using Social Media Responsibly
Guidelines for Staff in Schools

What is this guidance for?
The purpose of this guidance is to outline the responsibilities and expected standards of behaviour for all staff when using social media both inside and outside of work. It forms part of the school's existing ICT policies.

What is social media?
Social media is websites and applications that enable users to create and share content or to participate in social networking.

What role does social media have in school?
In school, communication is encouraged amongst our employees, children and parents. Social media can be a great way to stimulate conversation and discussion as well as sharing information and consulting. There are legitimate activities when employees can use social media on the internet as part of their work, however they must do so appropriately, in line with these guidelines and the council's and school values. These guidelines are to protect you and the reputation of the school. They aren't meant to restrict your work or personal use of what is an important method of communication and engagement.

Can employees use social media at work for personal use?
Every school may take a different approach, and it is therefore important to understand what is allowed. The Governing Body at this school permits the use of internet and social media on work premises, outside of work time, but only in circumstances outlined in this policy. You should be clear as to when you can access these sites. This is usually outside normal working hours and must not interfere with your or others day-to-day duties. Personal access should not be in view of any pupils, and you are reminded to log out or 'lock' the screen immediately upon leaving your mobile phone or PC, even if only for a short while. Personal use must be in accordance with the following guidelines, failure to follow them could result in disciplinary action.

What about using social media sites when I'm not in work?
The Governing Body respects an employee's right to a private life. However, they must also ensure that confidentiality and the reputation of the school are protected.
Even if your social media activities take place outside of work, what you say can have consequences, all staff must ensure they maintain their professionalism when using these sites. Your personal activities must not undermine the school's reputation, your professional reputation, or create perceptions of impropriety in the school, or bring the school in to disrepute.

TOP 10 TIPS TO KEEP YOU SAFE WHEN USING SOCIAL MEDIA

1) Do not "speak" for the school unless you have express permission…

You should not "speak" for the school (disclose information, publish information, make commitments/comments or engage in activities on behalf of the school) unless you are specifically authorised to do so by the head teacher. Any online activities associated with work for the school should be discussed and approved in advance by your head teacher.

2) Keep confidential…

Data protection laws apply on-line as well as in other media. Avoid sharing any confidential information about or dealings with the school, Governors, other employees, and/or members of the public unless you have express permission from your head teacher. Similarly, copyright laws mean that placing images or text from a copyrighted source (e.g. extracts from publications, photos etc) without permission is likely to breach copyright. Avoid publishing anything you are unsure about or seek permission in advance. Ensure only first names of pupils are used and make yourself aware of the pupils who do not have parental permission to appear on social media.

3) Protect yourself from identity fraud...

Restrict the amount of personal information that you give out. Social networking websites and online forums allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords and can lead to identity fraud and breach of council/school security.

4) If you can be linked to the school act appropriately...

Where you are clearly identifiable as being an employee of the school and/or discuss your work or school business using social media, you must behave appropriately and in ways that are consistent with the school's values and policies, avoiding any activities which might bring the school into disrepute.

5) Remember that colleagues, prospective employers, parents and children may see your online information…

Whether you identify yourself as an employee of the school or not, think carefully about how much personal information you want to make public and make sure your profile and the information you post reflects how you want them to see you both personally and professionally.

Once published, it can be very difficult to remove information from the public domain. It can stay public for a long time, can be amended or copied by others, or even changed

to misrepresent your intended message. You can never assume that your entries are private. It is important that you familiarise yourself with privacy settings and fully understand the professional implications of whichever level of security you chose. It is recommended that you apply the highest privacy settings and regularly review them, as the website may alter the setting without your knowledge.

Ensure that anything you post is in accordance with the schools ICT Security Policy, the schools ICT Acceptable User Policy, and your code of conduct, including the GTCE Code of Conduct (for teachers).
Be aware that inappropriate or derogatory comments about colleagues, Governors, parents or children could potentially lead to gross misconduct, which could ultimately result in dismissal.

6) Consider contact with pupils and parents carefully

Ensure than any contact with pupils (current or former) is strictly within an educational context, if necessary at all. You are strongly advised not to accept pupils as "friends" (for example on Facebook). For your own protection, if you do liaise with pupils electronically, you are advised to do so using official school email accounts, or managed learning platforms, so that any communication is logged and can be monitored, and remains within the acceptable boundaries of that professional relationship. If you receive contact from a pupil (current or former), you are advised to inform your Head Teacher who will make a decision about informing their parent(s)/carer(s), as there are specific rules which apply to use and misuse of social media sites for young people.

If, despite your best efforts, a pupil (current or former) makes contact with you, you should let your Head Teacher or the school's E-Safety coordinator know and do not reciprocate this communication. Remember the boundaries of your professional relationship with pupils and ensure that your behaviour does not blur these boundaries.

7) Choose your 'friends' carefully

You may appear in photographs published by other people, and you may be identified without consent, for example by "tagging" on Facebook, so you are advised to be mindful of what photographs you appear in. You can remove your identification from such photographs but not the photograph itself. Your 'friends' may not have as rigorous security settings as you might choose for yourself.

If you find out that through no fault of your own, you have been identified in a way which might be in breach of these guidelines, you must take immediate steps to rectify the situation. For example, by contacting the person who published the information / image and asking them to remove it and also report it to the Head Teacher.

8) Stay legal

Stay within the law at all times. Be aware that confidentiality, libel, defamation, copyright and data protection laws apply on-line just as in any other media. Whether you identify yourself as an employee of the school or not, think carefully about the information you post. Remember you are personally liable for what you publish online.

9) Never make offensive or defamatory comments…

About anyone linked to the school. Don't use discriminatory remarks, personal insults, obscenity or behave in ways that would not be acceptable in the workplace which could bring the school into disrepute, break the law and leave you open to prosecution and/or disciplinary action.

10) If in doubt get advice…

If you are unsure about anything to do with social media it's always best to get advice from your Head Teacher before you publish. Alternatively, contact your Human Resource Consultant who will endeavour to assist you. Many sites have produced guidance on using their sites safely and responsibly.
Other relevant policy documents include the following:

- E-Safety Policy
- ICT Acceptable User policy
- Tameside Safeguarding Children Board - Guidance for Safe Working Practice for adults who work with children and young people

Copies can be obtained from your Head Teacher and/or Business Manager.

Author: Sue Moore, Mel Bradley, Suzi Collins Date: May 2015

Signed:

Chair of Governors:

Date:

Signed: Head Teacher

Date:

Review : Annually Date: Summer term 2016

Appendix B

Laptop User's Policy

Acceptable Use

The registered user is permitted to use the laptop for personal, non-business use provided the registered user adheres to the provisions of this Laptop/Mobile Device Users Agreement.

- Personal usage of the laptop must not conflict or interfere with the work requirements of the registered user and must not negatively impact upon the School or the LEA.
- The registered user must abide by relevant legislation and guidance. Such legislation will change over time and the registered user is responsible for keeping up to date with such changes and ensuring the laptop/mobile device is used lawfully.

Duty of care

The registered user must treat the laptop/mobile device with care, both in and out of school and must not:

- leave the laptop/mobile device unattended and logged in.

- leave the laptop/mobile device unattended in a car or where it is vulnerable to theft or damage.

- take the laptop/mobile device out of the United Kingdom, unless on school business and additional insurance has been arranged in advance by the school.

- If the laptop/mobile device is lost/stolen or damaged through the registered user's negligence then the registered user is responsible for reimbursing the school any losses incurred for the replacement or repair of the laptop/mobile device. The registered user must inform the police and the head teacher of the school as soon as possible if the laptop/mobile device is stolen.

- All data stored on the laptop/mobile device is the responsibility of the registered user and the school cannot guarantee recovering lost or

deleted work from the laptop/mobile device. The registered user must back up his/her files on a regular basis.

- Under the Data Protection Act 1998 the school and the registered user have a responsibility for personal data relating to pupils and/or staff. If such personal data is to be held on the laptop/mobile device the registered user must ensure that it is protected by a password/pin and encrypted where relevant to prevent unauthorised access.

- The registered user must comply with the manufacturer's instructions for the use of the laptop/mobile device.

Virus Protection/Firewall on laptops.

The registered user must notify the school if they considered the anti virus software on the laptop needs updating or if the registered user believes the laptop has been infected by a virus. Anti Virus software is the responsibility of the school and must be updated by the School.

Software / Hardware / Apps & Maintenance

- The registered user may purchase and/ or install additional software/Apps on the laptop/mobile device, from the internet or otherwise, provided it is authorised by the ICT technician.

- The registered user must comply with all applicable licences relating to all software/apps installed on the laptop/mobile device.

- The registered user may purchase and/or use their own hardware and peripheries with the laptop/mobile device, provided the registered user adheres to all manufacturers' instructions relating to such. Any hardware purchased by the registered user will remain the responsibility of the registered user.

- Maintenance of the laptop/mobile device is the responsibility of the school and the registered user must not make alternative maintenance arrangements.

Internet & email

- The registered user is permitted to access the internet and send and receive personal emails in their own time, provided the registered user complies with the provisions of the Acceptable Users Agreement.

- Registered users are reminded that they must read and adhere to the provisions of the E-safety policy and, in particular, registered users must not access the internet for visiting illegal sites; visiting sites which display materials which could be considered by colleagues to be offensive; accessing reviewing or obtaining material which could or would serve to bring the employer or the school into disrepute or amount to criminal or illegal activity or for any other purpose forbidden under the E-safety policy.

- If inappropriate material is accessed by accident the registered user must inform a member of the E-safety team.

- The Police will be informed immediately if illegal material is found on the registered users laptop/mobile device (whether or not the registered user is still employed by the school) and relevant Child Protection procedures will apply, if applicable.
- Registered users are reminded that they must not send e-mail messages that are abusive, defamatory, offensive, obscene or malicious; or which make improper or discriminatory reference to a person's race, colour, religion, sex, age, creed, national origin, disability or physique or which might be perceived as damaging or likely to damage the reputation of the Employer or the School.

Freedom of Information

The recipient must assist and cooperate with the school to enable the school to comply with its obligations to disclose information under the Freedom of Information Act 2000. The recipient must provide to the school, or allow the school to access all information held on the users laptop/mobile device on behalf of the school, including all information that is held or generated on behalf of the school pursuant to the recipient's contract of employment and which may be required in order to respond to a request for information. The recipient shall provide or allow access to such information within 5 working days of a request from the school (or within such other period as the school shall specify).

Disclaimers

The school shall not be liable to the registered user for any loss, damage, cost or expense of any nature arising out of, but not limited to, the following

- the loss of the registered user data arising from the withdrawal or malfunction of the laptop/mobile device or otherwise;

- The consequences of any inappropriate or unauthorized use of the laptop/mobile device by the registered user including use which is contrary to the Health and Safety guidelines;

    - Any financial or consequential loss caused or arising from the use of the laptop/mobile device.

    - Any costs incurred by the registered user if the registered user uses the laptop/mobile device to purchase any goods or services.

- Except that neither the school nor its employees excludes its liability for death or personal injury caused by negligible use of the laptop/mobile device.

I have read, understand and will comply with the Laptop Policy for use of the laptop loaned to me as identified and specified above.

ICT Acceptable User Policy

Policy Issue Record

Issue 1	Sept 2009	Reviewed March 2015
Issue 2	March 2012	

Appendix C

ICT Acceptable Usage Policy

Introduction

At Dowson we believe in the concept of lifelong learning and the idea that both adults and children learn new things every day. We aim to produce 21st century learners that are able to use ICT in a safe and effective way to support this learning.

Aims and Objectives

To ensure that the Internet is used effectively as a tool for teaching and learning;

- Internet access will be planned to enrich and extend learning activities. Access will be controlled using filtering software
- Pupils will be given clear objectives for Internet use
- Staff will select sites which will support the learning outcomes planned for the pupils
- Pupils will be educated in taking responsibility for Internet access. Different ways of accessing the information from the Internet will be used depending upon the nature of the material being accessed and the developmental age of the pupils:

- Access to the internet may be through a teacher (or staff member).
- Pupils may be given a suitable web page or a single website to access
- Older pupils will be taught to use suitable internet search engines.

ICT Procedures

All users (including the parents and carers of the pupils) must sign an Acceptable User Agreement before using ICT available at Dowson Primary School.

Internet

- Users must access the Internet using their own logon names and not those of another individual.
- The internet must only be used for professional or educational purposes in school time. Staff may use the internet for private use outside of school hours providing they follow the guidelines in this document.
- Children must be supervised at all times by a members of staff or an approved adult when using the internet.
- All children are made aware of how to use the internet safely and what the implications are if the rules are broken.
- Accidental access to inappropriate, abusive or racist material must be reported without delay to a member of staff and a note of the offending website address (URL) taken so that it can be blocked.
- Internet filtering software (FORTIGATE) is installed to restrict access, as far as possible, to inappropriate or offensive content. This is reviewed and updated regularly.
- Users must not disclose any information of a personal nature in an email or on the internet.
- All emails sent should be courteous and the tone of the language used is appropriate to the reader. No strong or racist language will be tolerated.
- Bullying, harassment or abuse of any kind via email or the internet will not be tolerated.
- If users are bullied, or offensive emails are received this must be reported immediately to a trusted adult or member of staff within the school. Evidence should not be destroyed, but kept for investigation purposes.
- All email attachments and downloads are automatically scanned before they can be opened.
- Children must seek permission before downloading any files from the internet.
- Restrictions are in place to deny unauthorised installation of software.
- All users will be made aware of copyright law and will acknowledge the source of any text, information or images copied from the internet.

Shared School Network

Staff

- Users must access the school network using their own login names and passwords. These must not be disclosed or shared.
- Staff are able to access pupil work from the pupils personal folders. Restrictions are in place to deny access to staffs' personal folders.
- Staff have a restricted staff folder inaccessible to other network users.
- Access to information contained in the cloud will also restricted by user access rights and restrictions.

Personal Use

The School has devoted time and effort into developing the ICT systems to assist you with school work. It is, however, recognised that there are times when you may want to use the systems for non-work related purposes, and in recognising this need the school permits you to use the system for personal use.

You must not allow personal use of system to interfere with your day to day duties.

You must not use school software for personal use unless the terms of the licence permit this. Microsoft Office and Internet Explorer are licensed for personal use.

Use of the system should at all times be strictly in accordance with the this policy. You must pay all costs associated with personal use at the school's current rates e.g. cost of paper.

Equipment siting

Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- Devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- Equipment is sited to avoid environmental damage from causes such as dust & heat;
- Users should not leave computes logged-in or mobile device left unattended and not locked if unauthorised access to the data held can be gained.

The same rules apply when accessing the school's ICT system or ICT data away from school, e.g. at a user's home or visiting another school.

All mobile devices must have a minimum of a "key lock" or "screen lock" in place to help protect unauthorised access.

Pupils

- Users must access the school network using only their own logins.
- Pupils have their own personal space which is only accessible by the pupil logged in and staff members.

All Users

- Software should not be installed, nor programmes downloaded from the internet without prior permission from the person responsible for managing the network. Restrictions are in place to prevent this.
- Computers, laptops, netbooks and tablet devices with a suspected or actual virus infection must be disconnected from the network and be reported immediately to the System Manager.
- Computers or Mobile devices must never be left 'logged on' and unattended.

- If a computer or mobile device is left for a short while, it must be locked to prevent unauthorised access.
- Computers must be 'logged off' and mobile devices locked after use.

The use of Mobile Devices

Mobile devices, whether owned by Dowson Primary School or owned by a Dowson Primary School employee must meet with the following requirement and follow the following practices before being allowed access to school's Google Cloud services, school data or school's wireless network. Any breaches will result in the mobile device being removed from the system and the employees' online accounts being suspended until further investigation.

Mobile Device requirements

- Devices must use the following Operating Systems: Android 2.2 or later, IOS 6.x or later, Windows 7 or Windows 8 or a secure version of Linux.
- If the device allows, it must be configured with a secure password or PIN number This password must not be the same as any other credentials used within the organization.
- With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

Mobile Device Practices.

- Sensitive or confidential data should not be stored on the schools Google cloud base services. None confidential or sensitive data may be stored on the cloud providing the recommended security advice is adhered to.

- Sensitive data may only be stored on encrypted pen drives or a secured area on the school network.

- Users must report all lost or stolen devices to Dowson Primary School IT immediately whether they are personal devices or owned by Dowson Primary school.
- If a user suspects that unauthorized access to shool's data has taken place via a mobile device the user must report the incident to Dowson Primary School's Management or IT department.
- Devices must not be "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load pirated software or illegal content onto their devices.
- Applications / Apps must only be installed from official platform-owner approved sources (Google play / iTunes). Installation of code from untrusted sources is forbidden when accessing documents from Dowson Primary School Google Cloud Service . If you are unsure if an application is from an approved source contact Dowson Primary School IT.
- Users must not merge personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the school's email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Dowson Primary School IT immediately.
- User must make sure they log out of their email accounts before leaving their computer or shutting down.
- Users must not use school computers to backup or synchronise device content such as media files unless such content is required for legitimate school purposes.

<u>Cameras, Video Equipment, Webcams and Removable Devices</u>

- Personal camera/video equipment must not be used in school or on school visits. School equipment is available for this purpose.
- All photographs and videos are wiped from the peripherals after each used and stored in a secure folder on the school network.

- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.
- Webcams must not be used for personal communication and should only be used with an adult present.
- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.
- Pen Drives/Removable devices must be approved by the Network Manager/ICT Technician and scanned for viruses before being connected to network.

School Website

- Staff are responsible for approving all content and images to be uploaded onto our school website prior to it being published.
- The school website is subject to frequent checks to ensure no material has been inadvertently posted, which might put children or staff at risk.
- Copyright must be respected.

- Full names must not be used to identify pupils portrayed on the website. Similarly, if a child is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When saving photographs to be used on the website, their file names must not contain full names of individuals.

Sanctions to be imposed

- Letters will be sent home to parents or carers if applicable.
- Users may be suspended from using the schools computers, internet, email and Google Cloud based services etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious circumstances.
- Legal action may be taken in extreme circumstances.

Disciplinary Implications

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the school and the individual(s) concerned and/or civil claims for damages.

Concluding statement.

We are aware of the need to review this policy on a regular basis so that we can keep up with advances in the technology coming into the school. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates. We will review this policy annually.

Author: John Goodier/Suzanne Moore Date: September 2009

Reviewed & updated: john Goodier/Suzanne Moore Date: March 2015

Signed:

Chair of Governors:……..……..

Date:……..

Signed: Head Teacher:……

Date: ……

To be reviewed yearly

Date Spring Term 2016

Appendix D

ICT Security Policy

Issue Record

Author: Sue Moore/John Goodier

Approved by Governing Body:

Issue 1: Reviewed:

ICT Security Policy

Introduction

The purpose of the Policy is to protect the institution's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of Dowson Primary School to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- ICT security training will be available to all staff
- Data access from the cloud is secure and adequate protection is in place to ensure and allow safe access to information from devices not owned or managed by the school.

Policy Objectives

- to ensure that children, staff, equipment and data are adequately protected against any action that could adversely affect the school;
- to ensure that users are aware of and fully comply with all relevant legislation;

Roles and Responsibilities

The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, roles and responsibilities are defined below.

Governing Body

The governing body has the ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters.

In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

Headteacher

The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.

The Headteacher is responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:

- Registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data.
- Registrations are observed with the school.

In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers, laptops at home and cloud computing where data is available on multiple devices. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 1998 and ensure that any device accessing information is adequately secured.

System (Network) Manager

The System Manager is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including

responsibility for controlling access to these assets and for defining and documenting the requisite level of protection.

The System Manager will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

In line with these responsibilities, the System Manager will be the official point of contact for ICT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT security occurring within the school. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

It is vital, therefore, that the System Manager is fully conversant with the ICT Security Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

<u>Users</u>

Users are those employees, pupils or authorised guests of the school who make use of the ICT system to support them in their work. All users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy. The school has an Acceptable Use Policy which summarises the responsibilities of users of the school's ICT systems.

Users are responsible for notifying the System Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Tameside MBC Internal Audit department.

Users are responsible for the equipment they use including:

- Physical security

- Virus updates
- Operating system updates
- Security of data
- Their own passwords.

Personal Mobile Devices

Mobile devices when requiring access to school data must not be 'jailbroken' or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

Management of the Policy

Sufficient resources should be allocated each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors by the Headteacher.

Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. This information is provided in the Acceptable User Policy.

In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:

- New staff will be issued with and have read the appropriate documentation relating to ICT security, and have signed Acceptable Usage Policy.
- Access rights to the system are granted to an individual user based upon their role and responsibilities within the school and are based upon access to data in relation to school policy.
- Access rights will be amended or withdrawn due to a change to responsibilities or termination of employment.

Physical Security

Location Access

Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended.

The System Manager must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

Equipment siting

Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- Devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- Equipment is sited to avoid environmental damage from causes such as dust & heat;

- Users have been instructed to avoid leaving computes logged-in or mobile device left unattended and not locked if unauthorised access to the data held can be gained.

The same rules apply when accessing the School's ICT System or ICT data away from school, e.g. at a User's home or visiting another school.

All mobile devices must have a minimum of a "key lock" or "screen lock" in place to help protect unauthorised access.

Inventory

The Headteacher, in accordance with the System Manager, shall ensure that an inventory of all ICT equipment is maintained and all items accounted for at least annually.

Legitimate Use

The school's ICT facilities must not be used in any way that breaks the law or breaches council standards.

Such breaches include, but are not limited to:

- Making, distributing or using unlicensed software or data;
- Making or sending threatening, offensive, or harassing messages;
- Creating, possessing or distributing obscene material;
- Unauthorised personal use of the school's computer facilities.

Private Hardware & Software

Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved by the Network System Manager.

Storing Confidential Data

Sensitive or confidential data should not be stored on the schools Google cloud base services. None confidential or sensitive data may be stored in the cloud providing the recommended security advice is adhered to as stated in the Acceptable User Policy. Sensitive data can also be stored on encrypted pen drives or a secured area on the school network.

All school online data must remain in the cloud and not downloaded to the users personal mobile device.

Authorisation

Only persons who have read and signed the Acceptable User Policy may use and make use of the ICT System.

Failure to establish the limits of any authorisation may result in the school being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.

Where ICT systems are available for use, messages are displayed by the ICT System regarding unauthorised use of the system.

Passwords

The level of password control will be defined by the System Manager/ICT Technician including the use of "time out" passwords where a terminal/PC is left unused for a defined period.

Passwords for staff users are changed every 90 days and old passwords cannot be be re-used.

Passwords should be memorised and not written down.

Passwords or screen saver protection should protect access to all ICT systems.

Mobile devices should be protected by a screen lock.

A password must be changed if a breach of security is suspected or if there is a possibility that such a breach could occur, such as:

- When a password holder leaves the school or is transferred to another post;

- Users must not reveal their password to anyone.
- Users who forget their password must request a password reset via System Manager.

Security of the network

Only devices approved by the Network Manager should be permitted to be connected to the network, either through wired or wireless connectivity.

Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA encryption.

Open Wireless Access Points must not be connected to the school's network.

Where encryption is applied to wireless networks, encryption keys should be kept secure and known only to the Network Manager and technical staff.

The use of Mobile Devices

Mobile devices, whether owned by Dowson Primary School or owned by employees are important tools. However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the school's data and IT infrastructure. This can subsequently lead to data leakage and system infection. Dowson Primary School has a requirement to protect its information assets in order to safeguard its staff, student and reputation.

All staff are made aware of the potential risk in relation to such devices and have read and signed the Acceptable Users Policy.

Encryption

All portable devices that hold sensitive information should be fully encrypted. Devices subject to encryption may include:

- Laptops
- USB Pen drives

Where encryption is not deemed possible (e.g. SD Memory Cards used in Digital Cameras, or privately owned mobile devices) any data deemed to be sensitive or personal should not be stored on these devices.

Filtering of the Internet

Access to the internet for children and staff should be filtered using Fortigate firewall/internet filter.

It is the responsibility of the ICT System Manager to monitor the effectiveness of filtering at the school and report issues to the Headteacher.

Where breaches of internet filtering have occurred, the ICT System Manager should inform the Headteacher and assess the risk of continued access.

Backups

In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the System Manager, dependent upon the importance and quantity of the data concerned.

Data essential for the day to day running and management of the school should be stored on the school's network.

Backups containing data that must be password protected. They should be stored away from the system to which they relate preferably off site.

Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

Operating System Patching

The System Manager will ensure that all machines defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems.

It's at the discretion of the System Manager as to which updates and security patches are applied.

Virus Protection

The school will use appropriate Anti-virus software for all school ICT systems.

All Users should take precautions to avoid malicious software that may destroy or corrupt data as stated in the Acceptable User Policy.

As stated in the Acceptable User Policy users are made aware that any device in the ICT system (PC, laptops, netbook) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the System Manager who must take appropriate action, including removing the source of infection.

The School and Governing body will not be held responsible for the loss of data due to unauthorised installation of software or the lending of a computer, laptop or mobile device to an unauthorised user.

The ICT System Manager is responsible for the treatment of any virus problems.

Any third-party laptops not normally connected to the school network must be checked by the System Manager for viruses and anti-virus software before being allowed to connect to the network.

The school will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

Pen drives/removable devices must be approved by the Network Manager and scanned for viruses' before being connected to the network.

Disposal of Equipment

The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal to be destroyed.

Prior to the transfer or disposal of any ICT equipment the ICT System Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. The school should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

Repair of Equipment

If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed, if possible, before leaving site. The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

Security Incidents

All suspected or actual breaches of ICT security shall be reported to the System Manager or the Headteacher in their absence, who should ensure a speedy and effective response be made. Including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

Many incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

It should be recognised that the school and its staff may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action had been taken to resolve the breach.

Acceptable Use Policy

The school's Acceptable Use Policy applies to all school staff, students and third parties who use these facilities. The policy covers the use of email, internet, services accessed through the internet and local file and network usage. The conditions of use are explained in the policy. All school staff accessing these facilities must be issued with a copy of the 'Acceptable User Policy' and other relevant documents and complete the user declaration attached to the policy. For all students, the school will ensure that the relevant 'Acceptable User Policy' document is issued and the consent form is completed by pupils and their parents. In addition, copies of the 'Acceptable Usage Policy' document and consent form will be issued to all visitors.

Disciplinary Implications

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the School and the individual(s) concerned and/or civil claims for damages.

Author: Sue Moore/John Goodier Date: April 2015

Signed:

Chair of Governors:

Date:

Signed: Head Teacher

Date:

Review : 3 Years Date: Spring Term 2018

Appendix E

Dear Parent/Carers,

At Dowson we use "Google Apps for Education" for our Pupils from year 3 upwards. This system, powered by Google, will provide Gmail to our Pupils, as well as a suite of other Google products such as Google Docs, Google Sites and a Student Forum which will enable them to better communicate, share, and collaborate. We will be joining over 8 million other schools that are already using Google Apps around the world.

We are excited to offer Google Apps as it represents an important step towards developing an effective and up to date approach to the new curriculum and learning. These tools will support the high levels of collaboration that is required in today's classroom and to prepare students with communication and collaboration skills for life.

What's included in Google Apps?

- Gmail provides email storage with extra security including restricted incoming and outgoing email access. Emails by pupils are restricted to within Dowson Primary School. These email communications are monitored and recorded.
- Google Calendar enables us to create and share school or class calendars.
- Google Docs lets pupils create and share documents, spreadsheets, presentations, drawings and forms. This also allows pupils to work together on projects simultaneously.
- Google Drive is a 30GB cloud storage space reducing the need for pen drives etc. to be brought into school.
- Google Sites makes it easy to collect, share, and publish all types of content in a single website.
- Student Forum which is an online discussion area for our Pupils and restricted to Dowson Primary School. These communications are monitored and recorded.

What are the benefits of Google Apps and what's included?

- Ease of access, Pupils can access Google Apps at anytime, anywhere. It is designed to work in any browser (Google Chrome, IE, Firefox etc.) and on any computer, android or iOS operating system. This enables access to your email, calendars, documents and forum from school or at home.
- Online storage means that no flash drives (memory sticks etc.) are required as documents and files are stored in Google Docs.
- Students can easily collaborate with students from other classes, working together on group projects.
- During collaborative work teachers can monitor progress of each child and provide instant feedback visible to the group or to the individual. This enhances teaching and learning and provides accurate assessment.
- Students can develop an online portfolio of work throughout their years at the school.
- Through websites, calendars, and email and the Student forum parents can stay informed about the latest assignments and activities.

Parental Permission

In order to keep you informed and also to comply with data protection legislation and Google's Terms of Service, we are required to get parental permission.

Within the Google Apps service:

- There will be no advertisements.
- No external email addresses can contact pupil accounts, and vice-versa.
- All email communication and comments within collaborative work are monitored.
- Work uploaded to Google Drive remains the property of the creator; it is not copied or kept by Google if it is removed by the creator.

User Access

Pupils will be shown how to log on and use the facilities within Google Apps.

Pupils will be provided with unique usernames and passwords. Parents/Carers are encouraged to explore Google Apps with their children by logging in together and accessing their school work stored in Google Apps.

Pupils will follow school policies for appropriate use when using Google Apps. The service is an extension of the school's own network.

Pupils know that the school has the right and ability to monitor user accounts for policy and e-safety purposes.

Summary for Parents

Pupils without parental permission will be unable to participate in any lessons across the curriculum using Google Apps. All email communication is archived and the school's Acceptable Use Policy will be enforced. School staff will monitor the use of Google Apps when pupils are at school. Parents/Carers are responsible for monitoring their child's use of applications when accessing Google Apps from home. Pupils are responsible for their own behaviour at all times.

We are excited to be bringing these tools to the school. Don't hesitate in asking for more information about this decision and how it will impact teaching, learning and communication. This letter can also be found on the school website under the Parents and Letters Home.

Regards,

Mrs J A Rathburn

Headteacher

I give permission for my child to use Google Apps.

Childs Name _____Date

Class _____

Signed _____ Date _____

……

I do not give permission for my child to use Google Apps.

Parent/Guardian

Childs Name _____ Date _____

Class _____

Signed _____ Date_____

Appendix F

June 2015

Acceptable Use Agreement for the Internet, Email and other technologies

Note: *Students do not currently have access to external or internal Email. This agreement is worded to cover a number of technologies that maybe introduced into the school at a later date.*

In order for pupils at **Dowson** to browse the Internet or make use of Email and other technologies, we require each child (and their parent or carer) to sign to show that they understand the importance of adhering to these strict rules:

- I will only use the internet when I have permission and I am supervised
- I will only send emails to people my teacher has approved. I understand that racist comments or bad language will not be tolerated, and my emails will be polite at all times. I will not use emails as a way to bully another child or adult.
- I will not give out my address, home or mobile telephone number, photograph or school name and address on the Internet or in an email. I will not give out personal details of another child or adult either.
- I agree never to meet someone I communicate with through email and I will tell a teacher, parent or carer straightaway if a stranger tries to contact me on the Internet or by email.
- I will tell my teacher straightaway if I come across any unsuitable pictures or information on the Internet by accident, or if anything makes me feel uncomfortable or upset.
- I will only use search engines or websites that have been chosen by a teacher. I will not try to access any inappropriate websites, chat rooms, Instant Messaging or social networking sites in school.
- I understand that I am not allowed to keep my mobile phone with me in school and that I must have a letter from my parent(s) requesting permission for me to have my phone in school and that it must be handed into the office and signed in and out.
- I agree not to use the camera on my phone to take pictures of people without their permission and understand that any form of bullying by text message is unacceptable and will not be tolerated. I will not accept any files sent by a stranger to my mobile phone via Bluetooth.

- I will not download any files from the Internet in school unless I have permission.

Pupil

I understand the rules above and agree to follow them. If I break any of these rules, I understand that:

1. A letter may be sent home;
2. I may be banned from using the Internet for a given period of time
3. More serious action may be taken against me.

Pupil Signature: _____ Date: _ _/_ _/_ _

Name _____ Class _____

Parent or Carer

I give permission for my child to use the Internet, email and other technologies in school. I understand that pupils will be held accountable for their own actions and agree to appropriate sanctions being imposed if the rules are broken. I am aware that some materials on the Internet may be offensive and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information.

I understand that if I/we wish my/our child to bring a mobile phone into school for use at the end of the day, that I/we must write a letter requesting permission for that and that my child will have to hand their phone into the school office and for it to be signed in and out.

Name of Pupil_____ Class _____

Parent/Carer Signature: _____

Name: _____

Parent/Carer Signature: _____

Name: _____

Date: _ _/_ _/_ _