WELL GREEN PRIMARY SCHOOL, HALE

ICT ACCEPTABLE USE AND E-SAFETY

POLICY DOCUMENT

WELL GREEN PRIMARY SCHOOL
***ICT AND ACCEPTABLE USE* POLICY**
REVIEWED May 2021

Contents

Appendices

The aim of this Acceptable Use/e- Safety Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner, as part of the statutory curriculum requirements. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access 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 ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, 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.

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy, as required.

School's Strategy

We understand the responsibility to educate our pupils on e-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.

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet and associated technologies. These strategies are as follows:

Roles and Responsibilities

As e-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 named e-Safety Co-ordinator in our school is the Computing Lead. All members of the school community have been made aware of who holds this post. It is the role of the e-

Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Trafford LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ e-Safety Co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school-child agreement, and behaviour (including the anti-bullying) policy and PHSE.

e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of staff meetings and notices.
- Details of the ongoing staff training programme can be found e-Safety Co-ordinator
- New staff receive information on the school's Acceptable Use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

We endeavour to embed e-Safety messages across the curriculum whenever the Internet and/or related technologies are used. The school Internet access will be designed for pupil and teaching use and will include filtering policies appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.

The e-Safety policy will be introduced to the pupils at the start of each school year. Upon entry to the school all children and their parents are asked to read and sign the Acceptable Use/e-Safety policy. This policy is available on the school website. This form will be stored in each child's file in the school office.

E-safety posters will be prominently displayed.

e-Safety in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum as well as through specially designated days, e.g. Safer Internet Day.
- 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 and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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 Childline/ CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- Pupils will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Pupils will report accidental accessing of inappropriate materials in accordance with school procedures.
- Pupils will use the Internet for educational purposes only.
- Pupils will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Pupils will never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's Acceptable Use policy.
- Pupils will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy.
- Staff are provided with a School's Website log-in and password. Laptops are password protected and these have to be re-entered after a fixed time. Staff ipads have a passcode. All staff change their passwords every six months.
- All pupils have an individual, unique log in. In order to monitor ipad usage, children are assigned a specific ipad for the duration of their time at Well Green Primary.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the e-Safety Co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or School Website, including ensuring that passwords are not shared and are changed periodically
- Due consideration should be given to security when logging into the School's Website to the browser/cache options (shared or private computer)
- Password security is of the utmost importance and must be maintained at all times. Staff will be reminded never to disclose their passwords to children. The abuse of passwords must be reported immediately to the e-Safety coordinator and recorded in the e-Safety log.

Managing the Internet

The Internet is an open communication medium, available to all, 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. The security of the school network relies on the central firewall implemented by **Trafford MBC**. No traffic shall enter or leave the TMBC Infrastructure without being explicitly permitted by the firewall. No traffic shall route directly between connected establishments unless it has been explicitly allowed to do so. Whenever any inappropriate use is detected it will be followed up.

- The school maintains children will have supervised access to Internet resources by a teacher through the school's fixed and mobile internet technology. Children are never left unattended in the Computing Suite.

- Staff will preview any recommended sites before use.
- If Internet research is set for homework, it is advised that parents check the sites and supervise the 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.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor all internet usage. This record is emailed to the Headteacher every month by Trafford MBC.
- Pupils and teachers will be provided with training in the area of Internet safety.
- Virus protection software will be used and updated on a regular basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- Pupils will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

Infrastructure

- Trafford MBC has a monitoring solution via their network where web-based activity is monitored and recorded.
- School Internet access is controlled through the LA's web filtering service.
- Well Green Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the e-safety Co-ordinator and the URL and content will be reported to the TMBC ICT service team.
- It is the responsibility of the school, by delegation to the network administrators, (TCN) to ensure that anti-virus protection is installed on all school machines. This automatically updates.
- Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It IS the school's responsibility to install or maintain virus protection on personal systems, via TCN.
- Pupils and staff are not permitted to download programs or files on school based technologies.
- If there are any issues related to viruses or anti-virus software, the e-Safety Co-ordinator should be informed.
- The school will work with the TMBC, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. The filtering solution is currently managed by TMBC to filter the Internet stream to the school.
- As a response to the recent cyber-attacks on the education sector our Computing Support with AGSB have decided to add an extra layer of protection for all our Primary school clients. They will now be performing weekly offline/air-gapped backups. Details below.

  2 external hard drives will be used to rotate on a weekly basis. Once the backup has been successfully run it will be unplugged from the network and stored in a safe place (preferably the school safe) creating an offline/air-gapped backup of crucial data. This will

mean that should the network ever be compromised there will be an offline/untouched backup of crucial data available to restore from.
The backups will need to be ran manually.

Social Networks, Filtering and Emerging Technologies

The school through Trafford MBC will block all access to social networking sites, such as Bebo, Facebook, My Space and Twitter. (Most have a minimum age of 13 specified). Students are always advised never to give out personal details of any kind which may identify them or their location.

Managing email

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

- The LA gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Pupils may only use approved, teacher supervised, e-mail accounts (which do not personally identify them) on the school system
- Pupils may only use the approved VLE email system within school.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This 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 email addresses.
- Staff will not exchange personal social networking addresses or use social networking sites to communicate directly with pupils.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to carbon copy (cc) the Head teacher or the e-Safety Co-ordinator.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform the e-Safety Co-ordinator if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing curriculum.
- Pupils will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Pupils will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Pupils will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Pupils will note that sending and receiving email attachments is subject to permission from their teacher.

- Pupils will only have access to discussion forums, messaging or other electronic communication forms that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

School Website

The primary purpose of Well Green Primary's website is to provide information. It enables us promote the school to prospective parents and pupils. It also allows us to share important information with our current pupils and parents.

- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- Website using facilities such as guestbooks, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details.
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without the parental permission. Video clips may be password protected.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

Mobile technologies

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

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a parent/ carer using their personal device.

- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- No image or sound recordings are to be made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- We do not provide mobile phones in school, however several staff have their own.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community, however this is not recommended.
- As the school provides mobile technologies for offsite visits and trips (ipads), only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- Ipads are collected from the locked cabinet in the Computing Suite by a teacher or teaching assistant just prior to the lesson. These are transported in boxes to the relevant classroom and are never left unattended.

Pupils' personal Mobile devices

Pupils are not allowed to have personal mobile devices in school without the express permission of the Headteacher. Using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy. Children are not allowed to use other gaming or mobile devices to communicate or message others at anytime on the school premises.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. 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 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.

Consent of adults who work at the school

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

Publishing pupil's images and work

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

- on the School's website

- 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)

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. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Only teachers and TAs have the authority to upload photographs to the School's website, with the approval of the Headteacher.

Storage of Images

- Images/films of children are stored on teacher's laptops (provided by school) or school equipment and devices like cameras and ipads.
- 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 Head teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/website.

Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes and never using images of children or adults.
- 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).

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- 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.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse Infringements and Sanctions

Complaints

- Complaints relating to e-Safety should be made to the e-Safety Co-ordinator or Head teacher. Incidents should be logged and the **Flowcharts for Managing an e-Safety Incident** should be followed (see appendix).

Inappropriate material

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

  e-Safety Co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety Co-ordinator, which may result in disciplinary action, including written warnings, withdrawal of access privileges and depending on the seriousness of the offence; investigation by the Head teacher/LA, immediate suspension, possibly leading to dismissal and involvement of the appropriate authorities for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct on the **Acceptable Use Agreement**

Support Structures

The school will inform pupils and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Equal Opportunities

Pupils with special or additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents/carers and pupils are actively encouraged to contribute to the school e-Safety policy by letter and by reporting unsuitable sites etc to the e-Safety Co-ordinator
- Parents/carers and children are asked to read through and sign Acceptable Use Policy/e-Safety policy
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on School's website)

The school disseminates information to parents relating to e-Safety where appropriate in the form of the School website and newsletter items.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, pupils and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003

- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- Keeping children safe in education: for schools and colleges 2016

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation
Staff have been involved in making/reviewing the e-Safety policy.

Review Procedure
There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them.

This policy will be reviewed every year and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix

Acceptable Use Agreement/Code of Conduct:
Staff, Governors and Visitors

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

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety Co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

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

User Signature

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

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

Full Name ..... (printed) Job .....

Appendix

Permission Form

Please review the attached school e-Safety rules, sign and return this permission form to the Headteacher, Mrs Markham.

Name of Pupil: _____

Class/Year: _____

Pupil

I agree to follow the school's e-Safety rules on the use of the Internet, email and other Internet-related technologies. I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Pupil's Signature: _____ Date:

Parent/Guardian

As the parent or legal guardian of the above pupil, I have read the e-Safety rules, discussed them with my child and also grant permission for my son or daughter or the child in my care to access the Internet, email and other Internet-related technologies. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

I accept the above paragraph □ **I do not accept the above paragraph** □
(Please tick as appropriate)

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the e-Safety rules relating to publishing children's work on the school website.

During school events, I understand that I may take pictures of my child, however photographs including other children, other than my child should not be downloaded to social media networks or websites and children's names should never be published or mentioned, so they can be identified.

I accept the above paragraphs □ **I do not accept the above paragraphs** □
(Please tick as appropriate)

Signature: _____ Date: _____

Address: _____ Telephone: _____

_____

Appendix

School Pupil e-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use the school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix

e-Safety Incident Log

Details of **ALL** e-Safety incidents to be recorded by the e-Safety Co-ordinator. This incident log will be monitored by the Head teacher.

Date and Time	Name of Pupil or Staff	Male or Female	Computer or Class	Details of Incident (including evidence)	Actions and Reasons

Staff Laptop Agreement

Dear Staff Member,

You have been issued with a laptop computer for your use during your employment at Well Green Primary School. You are responsible for the proper care and control of the equipment issued to you. Listed below are the requirements and suggestions for caring for and using the equipment.

Please sign at the bottom to show both receipt and understandings of these requirements and return it to the Computing Lead or school bursar. You will receive a photocopy and the other will remain with the office. Please be aware that is your laptop is lost or stolen, there may not be funds available to replace it immediately.

All staff must undertake reasonable precautions to protect the laptop and any data stored on it. Specifically:

1. The laptop is not to be left in a car at any time. This includes a locked boot. The school's insurance does not cover equipment stolen from cars.
2. It is strongly recommended that the laptop is not left on front or back seats of a car whilst in transit as laptops have been stolen from car seats at traffic lights.
3. If you are travelling by public transport keep laptop with you at all times.
4. If the laptop is accidently damaged in any way, the Computing Lead or Bursar is to be informed immediately.
5. All staff are subject to the Trafford Borough Council policies and procedures regarding the use of ICT.
6. Management of data is subject to the provisions of the Data Protection Act and the Freedom of Information Act.
7. The laptop is for your use only, on official school business, however we do understand that the laptop may also be used for personal use within compliance with the e-Safety policy.
8. There is no requirement for you to insure the laptop, but you should consider informing your home contents insurer that you have this equipment at home.
9. You should not store any data on this laptop in case of loss or theft leading to sensitive or confidential data being stolen.

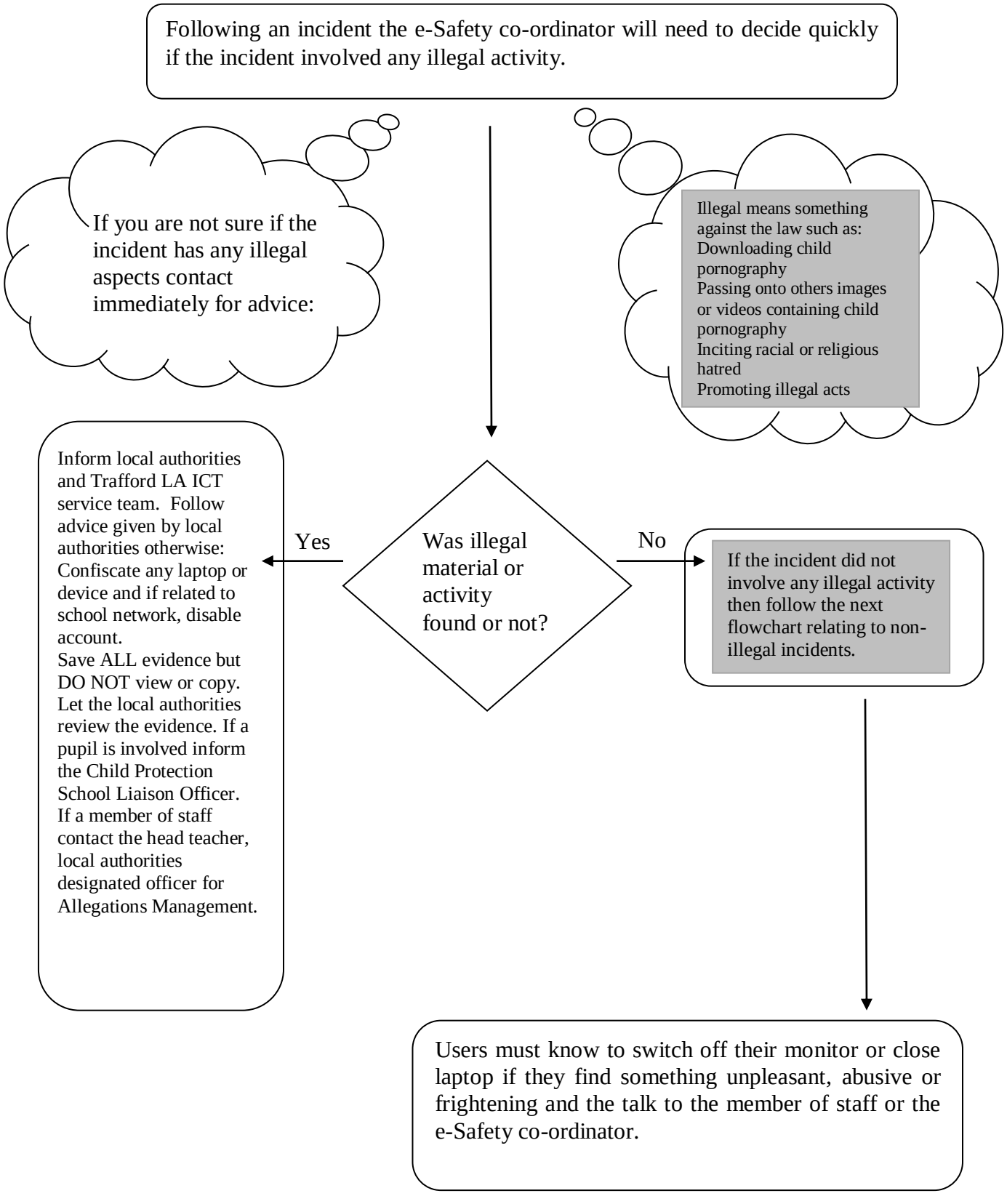
I undertake to return the laptop on termination of employment by the school, or when a reasonable request is made by the school to do so at any time.

Signed: ..... Date: .....

Model: ..... Serial Number: .....

Appendix

Flowchart for Managing and e-Safety Incident



Appendix

Flowchart for Managing and e-Safety Incident

If the incident did not involve any illegal activity then follow this flowchart.

The e-Safety Co-ordinator should:

- Record in the school e-Safety Incident Log
- Keep any evidence

Incident could be:

Using another person's username and password

Accessing websites which are against school policy

Using a mobile phone to take videos during lessons

Using the technology to upset or bully

Did the incident involve a member of staff?

Yes

If member of staff has:
Behaved in a way that has or may have harmed a child
Possibly committed a criminal offence
Behaved towards a child in a way which indicates s/he is unsuitable to work with children
Contact the LA if the incident does not satisfy the criteria in 10.1.1 of the HSCB procedures 2007 then follow points below.
Review evidence and determine if incident is accidental or deliberate.
Decide on appropriate course of action.
Follow school disciplinary procedures (if deliberate)

No

If the incident did not involve any illegal activity then follow this flowchart relating to non-illegal incidents.

Was the child the victim or the instigator?

Victim

In school action to support pupil by one or more of the following:
Class teacher
e-Safety Co-ordinator
Head teacher
Designated
Inform parent/carer as appropriate.
If child is at risk inform CSPLO immediately.

Instigator

Review the incident and identify if other pupils were involved

Decide appropriate sanctions based on school rules/guidelines

In serious incidents consider informing the CPSLO as the child instigator could be at risk

Review school procedures/policies to develop practice

Users must know to switch off their monitor or close laptop if they find something unpleasant, abusive or frightening and the talk to the member of staff or the e-Safety co-ordinator.

Appendix

Smile and Stay Safe Poster

e-Safety Rules to be displayed in school

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to e-Safety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual’s motivation, the Act makes it a criminal offence to gain:

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

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

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

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.