THE DOWNS
PREPARATORY SCHOOL
BRISTOL

Bertie's
NURSERY SCHOOL
Wraxall

G4.5 E-SAFETY & ACCEPTABLE USE OF ICT POLICY

Scope of the Policy

This policy applies to all members of the School (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of School ICT systems, both in and out of the School.

The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

This policy has been drawn up using guidance from the South West Grid for Learning (SWGfL) – www.swgfl.org.uk

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the School's e-safety provision. Children and young people need the help and support of the School to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.

- A planned e-safety curriculum should be provided as part of ICT and other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced in all ICT activities. Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

- It is recognised that mobile devices with 3G and 4G technology can provide unfiltered internet access. Pupils are not permitted to bring their own mobile devices into School unless specific permission has been given by the Head or Head of Prep School.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Technician can temporarily remove those sites from the filtered list or the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Some parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will therefore seek to provide information and awareness to parents and carers through curriculum activities, newsletters, Parents sessions and reference to the relevant web sites / publications e.g. www.swgfl.org.uk

Education & Training – Staff / Volunteers

It is essential that all teaching staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- Formal e-safety training will be made available to teaching staff. This will be regularly updated and reinforced. A review of the e-safety training needs of all staff will be carried out annually, via the appraisal system. It is expected that some staff will themselves identify e-safety as a training need.
- All new staff should receive e-safety awareness training as part of their induction programme, ensuring that they fully understand the School e-safety policy and where applicable, the Acceptable Use Agreements.
- The E-Safety Officer (or other nominated person) will monitor this policy and will present updates to staff via staff meetings / Inset days.
- The nominated governor responsible for safeguarding should have appropriate e-safety awareness, sufficient to monitor the School's implementation of the E-Safety Policy.

Technical – infrastructure / equipment, filtering and monitoring

The School will be responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the School meets recommended technical requirements.
- There will be termly reviews with the Head, Bursar, IT Technician and E-Safety Officer of the safety and security of school technical systems.
- Servers must be securely located and physical access restricted.
- All users will have clearly defined access rights to School technical systems and devices.
- All will be provided with a username and secure password by the IT Technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every academic year.
- The Administrator passwords for the School ICT system, used by the IT Technician must also be available to the Headmaster or Bursar and kept in a secure place (School safe).
- The IT Technician is responsible for ensuring that software licences are up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users of the School's main wifi system.
- The School has provided differentiated user-level filtering. Internet access is regulated by Censornet software. Antivirus software is in place (Sophos). The IT suites have classroom monitoring software provided by NetOp. Guest Wifi is available to adult visitors only, the password being supplied only by request from the School Office. The password is changed termly. (Sep17 – means of filtering this new network are now under review.)
- Mobile USB memory devices may not be used unless the files are password-protected and these files must not hold any personal data.
- School technical staff may monitor and record the activity of users on the School technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Guests/visitors are not permitted to access the School's main network systems without the prior consent of the E-Safety Officer.
- Network access codes must not be disclosed to any visitor without the consent of the IT Technician.
- Staff are not permitted to download executable files or install programmes on school devices without the prior consent of the IT Technician.

Password Security

All users of the School's ICT systems log in with an individual user name to ensure that all only have access to the data they have a right to access. The younger children in the PrePrep do use shared logons.
All staff passwords must meet the School's complexity requirements and are required to change at the beginning of every academic year.
Passwords should also be a minimum of eight characters and contain at least one upper case letter, one lower case letter and one number or symbol.

Users must not share their logon details with others or attempt to logon on using another user's account. The only exception to this is where two people job-share and therefore share a log-in. Before leaving a computer, all users must ensure that it is either locked or logged out, ensuring that nobody else can access their logon. All users are responsible for any activity that takes place under their user account.
Passwords must be changed as soon as there is any indication that they may be known by a third party.
User IDs and passwords of staff who have left the School's employment will be removed within 4 weeks.

School computers and mobile devices will be programmed to lock the screen after 15 minutes of inactivity.

School Issued Laptops and Tablets

Many staff are issued mobile computing devices. Their use is intended to support a member of staff's job role. Some personal use is permitted, provided that it does not interfere with its intended use.

Staff must not install new programmes without the permission of the IT Technician. It is acceptable to install updates of already-approved programmes.

All users are expected to treat any property that belongs to the School with respect and care. When devices are issued, the staff member is required to sign the Mobile Device Policy (Appendix 5 - Mobile Computing Devices Issued To Staff)

Any faults or breakages must be reported to the IT Technician as soon as possible. Staff are responsible for the safe-keeping of any device that has been issued to them and as such they must not :

- Leave a laptop or iPad unattended in an unlocked room unless its use is secured or it is locked in a cupboard
- Leave a School device in a public place unattended
- Use laptops on public transport or in other public places in order to protect personal safety and to avoid breaches of data protection.

All School-issued devices are insured, but should they be lost or damaged through negligence then users acknowledge that they will be liable for the cost of repair or replacement.

Social Media (Staff) - Protecting Professional Identity
(Staff should also refer to the Social Media Policy in the Employment Manual.)

The Downs School could be held responsible, indirectly for acts of its employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party.

Any breach of this policy may be treated as grounds for disciplinary action in accordance with the School's Disciplinary Procedure. This policy relates to the use of social media for both business and personal purposes during and outside normal school hours.

School staff should not :

- **Befriend a pupil or parent on social media sites.** The exception to this would be if the pupil or parent were a close personal friend or relative, in which case privacy settings must be arranged so that the site cannot be viewed by other pupils or parents.

School staff MUST NOT :

- **Post comments relating to or pictures of pupils nor those relating to School-related social outings or events.**
- Use their School email address for any use of social media.
- Use commentary deemed to be defamatory, derogatory or obscene.
- Attribute personal opinions to the School.
- Make reference in social media to students / pupils, parents / carers or School staff.
- Engage in online discussion on personal matters relating to members of the School community.
- Engage in online social media communications during working hours.
- Provide references for other individuals on social or professional networking sites as these may be attributed to the school and create legal liability for the author and the School.

School staff MUST :

- Wherever possible, ensure that privacy settings on social media sites are set so that pupils and third parties cannot access information relating to their personal lives
- Remove any postings that are deemed to constitute a breach of this policy
- Report to the Leadership Team any information on social networking sites that reflects poorly on the School
- Obtain written approval from the Headmaster, prior to the creation of any social media account or site that purports to represent The Downs School
- Amend their personal profiles with regard to their employment details immediately upon leaving the School

The IT resources and systems are the property of the School and as such, staff should have no expectation of privacy in any message, file, data, communication that has been transmitted using our systems. The School reserves the right to monitor, intercept and review staff activities using our systems to ensure that policies are being adhered to.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events

for their own personal use when permitted (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff must not be used.
- **Staff MUST NOT take images of pupils on their mobile phones.**
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs unless express permission is held
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. A consent form is usually obtained when the pupil is first admitted to the School.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

The contents of ICT resources are the property of the School and users can have no expectation of privacy in any electronic communication made via school systems. The School therefore reserves the right to monitor, intercept and review staff activities.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. Staff will report any concerns to the E-Safety Officer in the first instance and these may be recorded in the Child Protection file.

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (in Appendix 2) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Monitoring & Evaluation

The policy will be reviewed annually by the Bursar and the E-Safety officer in collaboration with the IT Technician, in the light of any reported incidents for concern, DfE guidance and that of other relevant bodies, and changes to the School's ICT provision. Revisions will be considered at the termly IT meeting with the Head.

The School's Risk and regulatory Committee will oversee updates to this policy via the annual review of safeguarding.

This policy was adopted on	Signed on behalf of the School
06/03/18	*H Walker*

Appendix 1

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the School.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Risk and Regulatory Committee receiving information about e-safety incidents and monitoring reports. A member of the Governing Body has the role of E-Safety Governor. (This is usually a combined role with that of the Child Protection / Safeguarding Governor). The E-Safety Governor will receive reports of e-safety incidents from the Designated Safeguarding Lead and will report to the Board where appropriate.

Headmaster / Leadership Team

The Headmaster has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
The Headmaster and the Bursar should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – Appendix 2 – "Responding to incidents of misuse").
The Leadership Team is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety Officer (This role is currently held by the School's Bursar for both The Downs School and Bertie's Nursery)

The E-Safety Officer :

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- sources training and advice for staff
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports to the E-Safety Governor on current issues, and to advise of e-safety incidents
- attends meetings of Governors where appropriate
- reports regularly to Leadership Team

IT Technician

The ICT Technician is responsible for ensuring that :

- the School's technical infrastructure is secure and is not open to misuse or malicious attack
- the School meets required e-safety technical requirements
- users may only access the networks and devices through officially issued user
- the filtering systems are applied and updated on a regular basis
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer for investigation / action / sanction
- that monitoring software / systems are implemented

Teaching Staff

Teaching staff are responsible for ensuring that:

- where staff take photographic images of children at school; they must use school equipment and use their professional responsibility in using, storing, sharing with parents and any school purpose, which may include Instagram, Twitter and the School website
- they have an up to date awareness of e-safety matters and of the current School e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to E-Safety Officer for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems, and only on school-owned equipment
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (DSL)

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

Pupils :

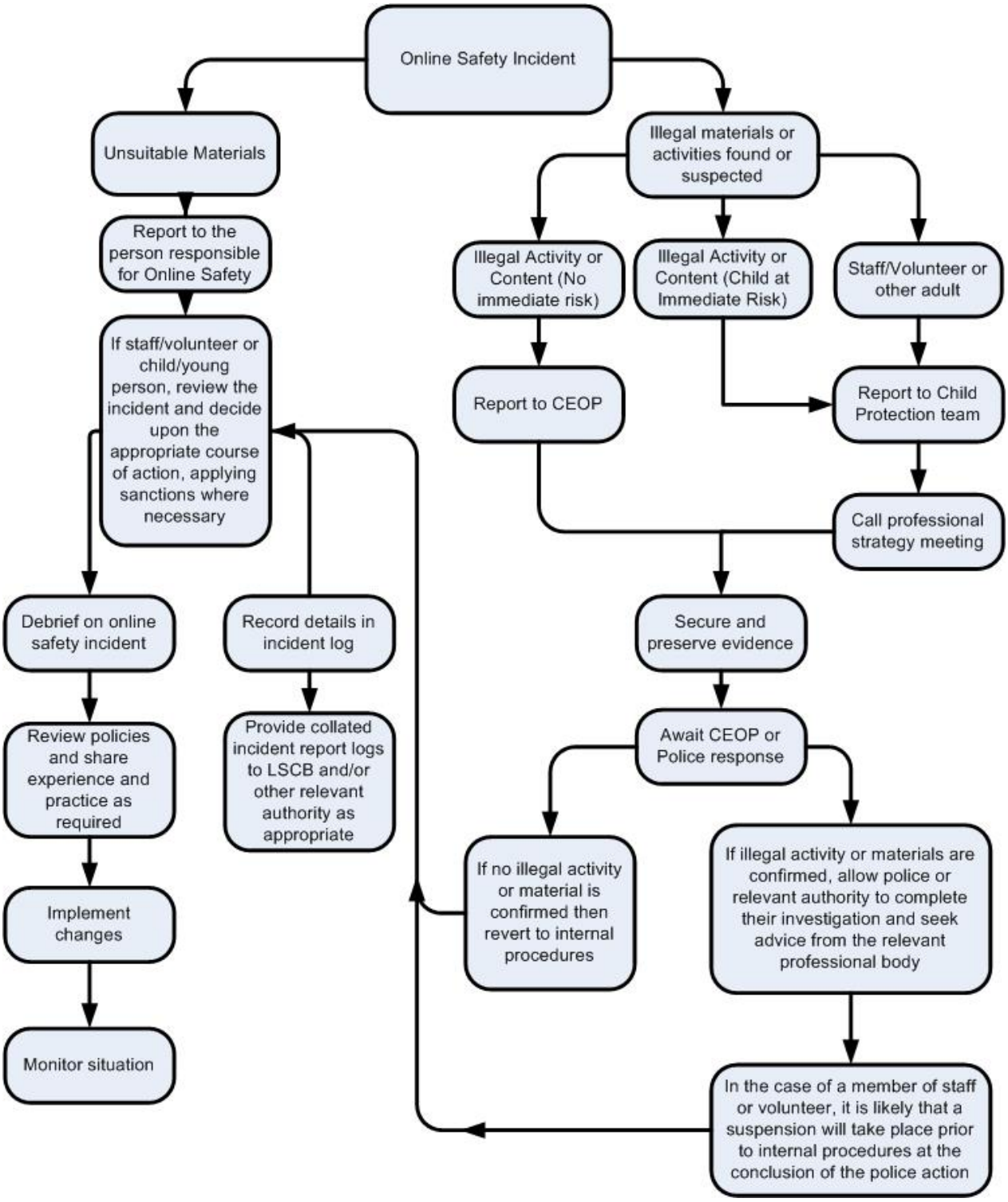
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so .
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the School.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will help parents understand these issues through parents' evenings, newsletters, and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

Appendix 2

Incidents of Misuse



Appendix 2 cont.

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Appendix 3 (a)

E-Safety & Acceptable Use of ICT Policy

Pupil Acceptable Use Agreement – For Pupils in Year 6, 7 and 8

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The E-Safety Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The School will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age etc)
- I will not arrange to meet people that I have met online.
- I will immediately report to a teacher any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the School systems and devices are for educational use and that I will not use them for personal use unless I have permission.
- I will not make downloads or uploads that might take up space on the computer or on the internet capacity and prevent other users from being able to carry out their work unless I have specific permission.
- I will not use the School systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).
- I will only print my work if I have specific permission.

- I will ensure that my hands are clean before using a device and I will not have any food or drink near any device.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise change any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the School has a responsibility to maintain the security of the technology it offers me and to ensure the smooth running of the School :

- I will not use my own personal devices (mobile phones / USB devices etc) in school unless I have specific permission. I understand that, if I do use my own devices in the School I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites whilst at School.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Pupil Acceptable Use Agreement **(For Pupils in Years 6, 7 and 8)**

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the Agreement and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school.

Name of Pupil	
Signed	
Date	

Parent / Carer Countersignature (optional)

Appendix 3 (b)

Pupil Acceptable Use Agreement **(For Pupils in Year 3, 4 and 5)**

- I will only use ICT in school for school purposes.
- I will only use my own school e-mail address when e-mailing.
- I will only open e-mails and email attachments and hyperlinks from people I know, or when my teacher tells me that I can.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone that I have met online.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

We have discussed this and …….....(child name) agrees to follow the E-Safety rules and to support the safe use of ICT at The Downs School.

Parent/ Carer Signature ……..…….

Date ……

Appendix 3 (c) **(For PrePrep Pupils to Year 2)**

E-Safety & Acceptable Use of ICT Policy

Pupil Acceptable Use Agreement (PrePrep)

This is how we stay safe when we use computers:

I will ask a teacher if I want to use the computers.

I will make sure my hands are clean before I use a computer.

I will only use activities that a teacher has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher if I see something that upsets me on the screen.

I will print my work only when the teacher tells me that I can.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……
(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent): ……..

Date ……..

Appendix 4 - E-Safety & Acceptable Use of ICT Policy

Staff (and Volunteer) Acceptable Use Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the School.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems, noting that when accompanying sports teams on away matches, I may exceptionally provide my personal mobile number in case of urgent need. All such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have consent from the IT department.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed

necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school :

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Appendix 5

The Downs School

Mobile Computing Devices issued to Staff

This agreement should be read in conjunction with the E-Safety Policy (Staff Handbook) and Data Protection Policy (Employment Handbook).

Ownership
The device remains the property of The Downs School at all times.

Configuration
All laptop and desktop computers provided will be Windows-based products. The computers will have a standard range of software applications installed and will be configured to operate on the School network both wirelessly and using built in Ethernet.

New software may only be installed with the permission of the IT Technician.

Any non-standard software that interferes with the operation of the computer will be removed. Should the user change the configuration and a problem occur, the laptop will be restored to the standard configuration. Any configuration changes to the device to enable it to work outside The Downs School are the responsibility of the user. The user must ensure that he or she has a record of all relevant user names, passwords, serial numbers, etc. because in the event of a problem, the laptop will be restored to the standard configuration.

Use
The device is provided for the member of staff to use and no one else, and only in connection with their employment at The Downs School. Nothing must be done to the device that prevents this. This includes but is not restricted to:

- Filling the hard disk with personal data, thus preventing The Downs School material from being stored.
- Installing any item of hardware or software that interferes with the operation of the laptop.
- Changing the network settings.

The device, and The Downs School network, must **not** be used to store illegal material **nor** be used for any illegal or inappropriate activity, such as gambling, surfing for pornography, or for sending abusive or inappropriate e-mails. Disciplinary action will be taken in the event of a breach of this clause.

Backing up data
The user is responsible for backing up any data on the device. School facilities exist for the backing up of The Downs School related data. The user is responsible for backing up personal data. If you are unsure of how to safely back-up any data, please consult the IT Technician.

Care & Security

The user must take good care of the device and may be **personally liable** for any costs incurred due to negligent damage to the device e.g. dropping, defacing, spilling drink or food onto the laptop.

Staff are responsible for the safe-keeping of any device that has been issued to them.and as such they must not :

- Leave a laptop or iPad unattended in an unlocked
- room unless its use is secured or it is locked in a cupboard
- Leave a School device in a public place unattended
- Use laptops on public transport or in other public places in order to protect personal safety and to avoid breaches of data protection.
- Devices must not be left in any motor vehicle other than out of sight in a locked boot. Under no circumstances should a device be left in a motor vehicle between the hours of dusk and dawn unless the vehicle is stored in a locked garage. These are conditions of the school's insurance policy and failure to adhere to them will result in cover for any incident being declined by the school's insurers and the member of staff would be **personally liable** for the loss.

As the device may be reissued to another member of staff, the user must not write on or mark the device, or attach or stick anything onto the device.

The user must make sure that they wash their hands if they use their fingers to erase marker pen marks on a white board. The cleaning fluid used to clean the whiteboards transfers from fingertips and over a period of time erases the letters on the keyboard. N.B. other products can have the same effect, e.g. perfume/after-shave.

Access Controls

Passwords and identifications must be kept confidential and may not be shared or revealed to colleagues or third parties under any circumstances.

Passwords must be changed annually and immediately if there is a suspicion that a third party may have discovered a password. Passwords must comply with the complexity requirements of the E-Safety Policy.

Staff Declaration

I have read and fully understood the Downs School Mobile Device Issue Agreement and agree to abide by its terms.

I have been issued with the equipment detailed below and agree to return it on request or at the end of my employment with the school.

Name _____

Signature _____ **Date** _____

Mobile Device Model _____ **Serial Number** _____

This policy was adopted on	Signed on behalf of the School	Date for review
06.03.18	*HLW*	*01.02.19*