DOWNSVIEW PRIMARY SCHOOL

E-SAFETY POLICY

Originator: M. Harrison

Adopted on: 5th September 2016

Revision Date: September 2017

Downsview Primary School
Biggin Way
Upper Norwood
London
SE19 3XE

Telephone: 020 8764 4611
Email: sec1@downsview.croydon.sch.uk
Website: www.downsview.croydon.sch.uk

Downsview E-Safety Policy 2016

(Read in conjunction with Teaching & Learning, Safeguarding, Computing, Devices and PSHE Policies)

The main purpose of this policy is to ensure that members of staff, pupils and the wider school community understand the approach Downsview takes to e-safety and the steps we take to minimise any risks that may be found in the modern world. The curriculum at Downsview is designed to educate pupils whilst opportunities are given to staff, parents and carers to participate and update their own e-safety awareness.

The E-Safety Policy will be reviewed annually, or when any significant changes occur with regard to the technologies in use within the school. There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team and approved by Governors. All amendments to the school E-Safety Policy will be disseminated to all members of staff and pupils.

Aims

- To ensure the school is in line with statutory requirements.
- To give all members of the school community a clear understanding of e-safety.
- To give children and adults the tools to use the internet safely.
- To minimise the risk of children and adults being exposed to inappropriate content on the web.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• **Must be adequately trained in off-line and online safeguarding, in line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance.** • To lead a 'safeguarding' culture, ensuring that e-safety is fully integrated with whole school safeguarding. • To take overall responsibility for e-safety provision. • To take overall responsibility for data management and information security (SIRO), ensuring school's provision follows best practice in information handling. • To ensure the school uses appropriate IT systems and services, including filtered Internet Service, e.g. LGfL services. • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and e-safety roles. • To be aware of procedures to be followed in the event of a serious e-safety incident. • Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised.

Role	Key Responsibilities
	• To receive regular monitoring reports from the Computing and E-Safety Leader. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures, e.g. network manager. • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for e-safety. • To ensure the school website includes relevant information.
Computing and E-Safety Leader	• Take day to day responsibility for e-safety issues and a leading role in establishing and reviewing the school's E-Safety Policy and documents. • Promote an awareness and commitment to e-safety throughout the school community. • Ensure that e-safety education is embedded within the curriculum. • Liaise with school technical staff where appropriate. • To communicate regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs and filtering/change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident relating to both children and/or staff. • To ensure that e-safety incidents are logged, where appropriate, as a safeguarding incident and are forwarded to SLT. • Facilitate training and advice for all staff. • Oversee any pupil surveys and pupil feedback on e-safety issues. • Liaise with the Local Authority and relevant agencies. • Is regularly updated on e-safety issues and legislation, and aware of the potential for serious child protection concerns. • To oversee the delivery of the e-safety element of the Computing curriculum.
Governors: Safeguarding governor (including e-safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online. • To review the effectiveness of the policy and seek approval from the Full Governing Body to adopt the E-Safety Policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the E-Safety Governor will include: regular review with

Role	Key Responsibilities
	the Computing and E-Safety Leader.
Network Manager/technician	• To report e-safety related issues that come to their attention, to the Computing and E-Safety Leader. • To manage the school's computer systems, ensuring:- - school password policy is strictly adhered to; - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date); - access controls/encryption exist to protect personal and sensitive information held on school-owned devices; - the school's policy on web filtering is applied and updated on a regular basis. • To keep up to date with the school's E-safety Policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Computing and E-Safety Leader and Headteacher, when appropriate. • To ensure appropriate backup procedures and disaster recovery plans are in place. • To keep up-to-date documentation of the school's online security and technical procedures.
Data and Information (Asset Owners) Managers (IAOs)	• To ensure that the data they manage is accurate and up-to-date. • To ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted, in-line with data protection requirements. • The school must be registered with the Information Commissioner's Office.
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school, following data handling procedures as relevant.
Teachers	• To embed e-safety in the curriculum. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities, if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content. such as copyright laws.

Role	**Key Responsibilities**
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the Computing and E-Safety Leader. • To maintain an awareness of current e-safety issues and guidance through CPD, Staff Meetings and INSET. • To model safe, responsible and professional behaviours in their own use of technology. Exit strategy • At the end of the period of employment, to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset
Pupils	• To read, understand, sign and adhere to the Pupil Acceptable Use Policy annually. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they, or someone they know, feels worried or vulnerable when using online technology. • To understand the importance of adopting safe behaviours and 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. • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences.
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology. • **To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement, which includes the pupils' use of the Internet and the school's use of photographic and video images.**
External groups, including Parent groups	• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within school. • To support the school in promoting e-safety. • To model safe, responsible and positive behaviours in their own use

Role	Key Responsibilities
	of technology.

Communication:

The policy will be communicated to staff, pupils and the school community in the following ways:

- Policy to be posted on the school website and staffroom. A hard copy will be presented to staff in September.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on e-safety for all staff.
- Acceptable Use Agreements discussed with staff and pupils at the start of each year. Acceptable Use Agreements to be issued to whole school community, on entry to the school.

Education and Curriculum

Pupil e-safety curriculum

Downsview has a clear and progressive e-safety education programme as part of the Computing and PSHE curriculum (App. 1) and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience. The curriculum has been planned out to cover a broad range of e-safety aspects. The curriculum will review and remind students about their responsibilities through the pupil Acceptable Use Agreement(s).

Staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, for example the use of passwords, logging-off, use of content, research skills, copyright; this is updated through staff training.

The E-Safety curriculum ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

Across the curriculum, it is ensured that pupils only use school-approved systems and work within appropriately secure / age-appropriate environments.

The Prevent Duty is taught as an element of the e-safety curriculum across the school.

Staff and governor training

Downsview makes regular training available to staff on e-safety issues and the school's e-safety education programme, It also provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the E-Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

Downsview provides E-Safety Workshops for parents, which includes online safety and runs a rolling programme of e-safety advice, guidance and training for parents.

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems, in accordance with the relevant Acceptable Use Agreements (App. 2/3);
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good e-safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices, including cameras;

Staff, volunteers and contractors

All adults at Downsview should be vigilant in the supervision of children at all times, as far as is reasonable, and use common-sense strategies in learning resource areas, where older pupils have more flexible access; know to take professional, reasonable precautions when working with pupils, previewing websites before use; using guided, age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Parents/Carers

Parents and Carers should provide consent for pupils to use the Internet, as well as other technologies, as part of the E-safety Acceptable Use Agreement form to support children in the curriculum.

Parents and Carers should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse as stated below.

Incident Management

Handling Incidents

The school will take all reasonable precautions to ensure online safety. Staff and pupils are given information about infringements and possible sanctions. Computing and E-Safety Leader acts as first point of contact for any incident.

Any suspected online risk or infringement is reported to Computing and E-Safety Leader that day. Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). For more information, see below.

At Downsivew, there is strict monitoring and application of the E-safety Policy and a differentiated and appropriate range of sanctions.

All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;

- Any e-safety incident should be reported to the Computing and E-Safety Leader. They will then refer the incident to the appropriate member of staff or SLT. App. 4 gives examples of different e-safety scenarios and, if appropriate, the escalation process.
- An E-Safety Log (App. 5) will be completed for incidents ranked at green and above on our system.
- Parents/carers are specifically informed of e-safety incidents involving young people, for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law; support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with e-safety issues.
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.
- Monitoring and reporting of e-safety incidents take place and contribute to developments in policy and practice in e-safety within the school.

Managing IT and Communication System

Internet access, security (virus protection) and filtering

All users at Downsview are informed that Internet and e-mail use is monitored.

Downsview has the educational filtered secure broadband connectivity through the LGfL and uses the LGfL filtering system, which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status. Downsview also uses USO user-level filtering where relevant; Network health is checked and maintained through use of Sophos anti-virus software (from LGfL);

Downsview uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

Downsview continues to work in partnership with the LGfL and its technical support provider to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network Management (user access, backup)

Downsview uses individual, audited log-ins for all users - the LGfL USO system. For external or short term visitors, Downsview uses guest accounts for temporary access to appropriate services.

Downsview uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful.

Where appropriate, Downsview has additional local network monitoring/auditing software installed.

Downsview and Downsview's technical support provider ensures the Systems Administrator and network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies.

Downsview uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance; the storage of all data within the school will conform to the EU and UK data protection requirements; storage of data online, will conform to the EU data protection directive where storage is hosted within the EU. The system has daily back-up of school data (admin and curriculum).

To ensure the network is used safely, Downsview:

Ensures staff read and sign that they have understood the school's Acceptable Use Policy. Following this, they are set-up with Internet, e-mail access and network access. Online access to service is through a unique, audited username and password. Staff will also use the same username and password for access to our school's network.

All pupils have access to a unique class username and password which gives them access to the Internet and other services; staff and pupils should not log on as another user - pupils should never be allowed to log-on or use teacher and staff logins. During school, it is required all users to log off when they have finished working or are leaving the computer unattended.

Downsview has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.

Downsview, where appropriate, ensures all equipment owned by the school has up to date virus protection.

This policy makes clear that staff are responsible for ensuring any computer or laptop loaned to them by the school, is only used to support their professional responsibilities.

Downsivew ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems: It does not allow any outside agencies to access our network remotely, except where there is a clear professional need.

The wireless network has been secured to industry standard security level and follows appropriate standards suitable for educational use.

Password policy

This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private, unless required by administration purposes.

In the case of shared systems, such as cloud storage, logins and passwords may be shared with those who need access to specific accounts.

E-mail

Downsview provides staff with an e-mail account for their professional use and makes clear personal e-mail should be through a separate account; e-mail accounts should not be used to send or receive personal e-mails. Downsview will ensure that e-mail accounts are maintained and up to date. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct e-mail filtering for viruses.

Downsview will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

Staff should never use e-mail to transfer staff or pupil personal data. Staff should use professional judgement when sending school related documents, even to share with colleagues.

There is no requirement for students to have personalised school e-mails.

School website

The Headteacher, supported by the Governing Body and selected members of staff, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school website complies with statutory DFE requirements.

Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status.

Photographs published on the web do not have full names attached. We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website.

Social networking

Staff, Volunteers and Contractors

Staff are instructed to always keep professional and private communication separate. Teachers are instructed not to run social network sites as a means of communication with students or parents. School staff should not be on-line friends with any pupil/student. Any exceptions must be approved by the Headteacher.

In private use, staff will ensure no reference should be made in social media to pupils, parents/carers or school staff. Staff do not engage in online discussion on personal matters relating to members of the school community; Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information and to ensure content that is public is appropriate.

Downsview uses Social Networking to update parents and carers and as a running news feed. Parents and carers may opt out of their children appearing in such media by writing in to the school.

Pupils:

Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our e-safety curriculum work. Pupils are required to sign and follow our pupil Acceptable Use Agreement. Pupils are deterred from using Social Media until they reach the legal age of requirement.

Parents:

Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials, when required. Parents are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Cloud Environments

Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities, e.g. all class teachers upload information in their class areas; photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.

In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Staff are prohibited from using USBs, external hard drives or personal cloud storage as this can cause a risk to the system or transfer sensitive data. All staff have access to school based cloud systems which can be used to transfer appropriate data and information.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At Downsivew, the Head Teacher is the Senior Information Risk Officer (SIRO).

Staff are clear who are the key contact(s) for key school information (the Information Asset Owners). We have listed the information and information asset owners.

We ensure staff know who to report any incidents, where data protection may have been compromised.

All staff are DBS checked and records are held in a Single Central Record.

Technical Solutions

Staff have secure area(s) on the network to store sensitive files. Downsview requires staff to log-out of systems when leaving their computer. LGfL USO AutoUpdate is used for creation of online user accounts for access to broadband services and the LGfL content.

All servers are in lockable locations and managed by DBS-checked staff.

Details of all school-owned hardware will be recorded in a hardware inventory. Software is monitored across devices to ensure that it is in line with school policies.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

	Aut. 1	**Aut. 2**	**Spr. 1**	**Spr. 2**	**Sum. 1**	**Sum. 2**
Nursery	N/A	N/A	N/A	N/A	N/A	**N/A**
Reception	**ES:** E-Safety basics – introducing the poster	**ES:** Technology at school	**ES:** Safe internet use	**ES:**	**ES:** Technology at home	**ES:** Safe image searching – what to do.
Year 1	**ES:** E-Safety basics – chn's knowledge	**ES:** Using technology safely (DL)	**ES:** Using the internet safely (DL)	**ES:** Personal Information (e.g. Mathletics) (DL)	**ES:** Personal Information (e.g. online games) (DL)	**ES:** Sharing online
Year 2	**ES:** E-Safety basics – chn's knowledge	**ES:** Using technology respectfully (DL)	**ES:** Reporting concerns (DL)	**ES:** Reporting concerns – 1,2,3,4 approach (DL)	**ES:** Purpose of technology out of school (DL)	**ES:** Purpose of technology in school (DL)
Year 3	**ES:** E-Safety basics – chn's knowledge	**ES:** Using technology responsibly (DL)	**ES:** using the web (DL)	**ES:** using the services the web provides (DL)	**ES:** Getting help/ reporting -SMART steps	**ES:** Does technology always achieve my goals?
Year 4	**ES:** E-Safety basics – chn's knowledge	**ES:** Getting help/ reporting - SMART steps	**ES:** Acceptable behaviour using technology (DL)	**ES:** Unacceptable behaviour using technology (DL)	**ES:** Safe searching on the web	**ES:** Selecting correct information
Year 5	**ES:** E-Safety basics – chn's knowledge	**ES:** Online profile	**ES:** Making choices on the web (DL)	**ES:** Understanding that not everything is true/safe – ranked results (IT/DL)	**ES:** Safe communicating	**ES:** Reporting (other medias)
Year 6	**ES:** E-Safety basics – chn's knowledge	**ES:** Online Risks	**ES:** Online Risks (DL)	**ES:** Minimising risks (DL)	**ES:** Copyright	**ES:** Social Media

App. 1 - E-Safety Curriculum and Useful Links

The following resources can be used as a tool to support E-Safety lesson plans:

BBC Bitesize - http://www.bbc.co.uk/education/topics/zcpp34j/resources/1

ThinkUKnow – http://www.thinkuknow.co.uk/

LGfL Resource Matrix - http://www.lgfl.net/esafety/Pages/Primary-resource-matrix.aspx

ChildNet Resources - http://www.childnet.com/resources

Google Legends - http://www.google.co.uk/safetycenter/families/legends/downloads-resources/

C – Computing ES – E-Safety CS – Computing Science/Algorithms and Programming DL – Digital Literacy IT – Information Technology

App. 2 Staff Acceptable Usage Policy

AUP review Date	**July 2016**
Date of next Review	**July 2017**
Who reviewed this AUP?	**Computing and E-Safety Leader**

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the E-Safety and any linked procedures in the Devices and Computing policy.
- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: *LGfL StaffMail*
- I will only use the approved *London Mail*, *Learning Platforms and school approved communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business. For more details, read the devices policy.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Computing and E-Safety Leader, Computing Impact Team or Finance Officer.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not use USBs, personal clouds or any other storage devices in school. If access to work related content is required, then I will use either remote access or school provided cloud systems.
- I will not connect any device, to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems.*
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Downsview's Computing and E-Safety Leader and/or child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the Computing and E-Safety Leader or a senior member of staff.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's e-safety policy and computing policy into my teaching.

Acceptable Use Policy (AUP): Agreement Form
All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a ‘safe and responsible digital technologies user’.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .... Date ....

Full Name .... (printed)

Job title / Role ....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature .... Date ....

Full Name .... (printed)

App. 3. Pupil Acceptable Usage Policies

Downsview KS1 Acceptable Use Policy 2016

Think before you click

S	I will only use the Internet with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don’t like on a screen, I will always tell an adult

My Name:

My Signature:

Downsview KS2 Acceptable Use Agreement 2016

These rules will keep me safe and help me to be fair to others.

- I will only use the school’s computers for schoolwork and homework.
- I will use the school’s computers and equipment sensibly. Look after it and make sure it is stored securely when I have finished using it.
- I will only edit or delete my own files and not look at, or change, other people’s files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

App. 4 – Downsview's Levels of E-Safety and Escalation Process

Category 1	Category 2	Category 3	Category 4	Category 5
Staff dealing with incident: Staff reporting incident **Informing:** Class teacher Computing and E-Safety Lead	**Staff dealing with incident:** Computing and E-Safety Lead Class teacher **Informing:** Head of Year	**Staff dealing with incident:** Computing and E-Safety Lead Head of Year/SLT **Informing:** SLT	**Staff dealing with incident:** Computing and E-Safety Lead SLT/Head **Informing:** Head/Governors	Staff dealing with incident: SLT/Head Governors Computing and E-Safety Lead **Informing:** Local Authority
Pupil related incident. **Example of incident:** Accidently viewing image through safe search that has offended the child.	**Pupil related incident.** **Example of incident:** Accidently viewing image through safe search that should not have gotten through filtering (e.g. nudity)	**Pupil related incident.** **Example of incident:** Sharing personal information. Cyberbullying**.**	**Pupil related incident.** **Example of incident:** Sharing and/or distributing inappropriate content. Repeated cyberbullying.	**Pupil related incident.** **Example of incident:** Seeking out inappropriate content such as pornography, terrorism, etc.
Staff related incident. **Example of incident:** Concerns over own Social Networking sites security	**Staff related incident.** **Example of incident:** Concern over messages received on school based social networking	**Staff related incident.** **Example of incident:** Contacting parents/carers with personal devices.	**Staff related incident.** **Example of incident:** Sharing of content between children and staff outside of school settings.	**Staff related incident.** **Example of incident:** Sharing of inappropriate content between children and staff.
		Parent/Carer related incident. **Example of incident:** Parents allowing students to use social media.	**Parent/Carer related incident.** **Example of incident:** Parents allowing students to be exposed to inappropriate age-rated content (e.g. games/films).	**Parent/Carer related incident.** **Example of incident:** Exposing children to inappropriate content such as pornography, terrorism etc.

All concerns can move up the scale depending on circumstances and urgency. Computing and E-Safety Leader should be first point of call for **ALL** incidents and will relay information to the appropriate members of staff once an outline of events has been established. Any e-safety issue identified as green or above must identified in an e-safety log.

App. 5 E-Safety Log

E-Safety Incident Log

Details of **ALL** e-safety incidents, green or above, to be recorded by the Computing and E-Safety Leader, Downsview's Technical Support or any other appropriate member of staff. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Date & Time	Name of pupil or staff member	Room and computer / device number	Details of incident (including evidence)	Actions	Name and role of person completing this entry

Details of first reviewing person (person reporting incident):

Name	
Position	
Signature	

Details of second reviewing person (person dealing with incident)

Name	
Position	
Signature	

Website(s) address / device	Reason for concern

Follow up action (if required)/Outcome:
