



Dropmore Infant School
Littleworth Road, Dropmore, Burnham
Buckinghamshire SL1 8PF
Telephone: 01753 644403

Headteacher: Mrs Gitta Streete

Chair of Governors: Mr Tim Wicks

Policy No: 042

Policy Title: E-Safety Policy

Issue No: 004

Effective Date: June 2020

Next Review Date: June 2021

Approved by Chair of Governors: 

Date: 30.06.2020

DROPMORE INFANT SCHOOL E-SAFETY POLICY

TABLE OF CONTENT

1. Policy and Leadership

1.1 Scope

1.2 Responsibilities

1.2.1 Governors

1.2.2 Headteacher

1.2.3 E-Safety coordinator

1.2.4 Network Manager

1.2.5 Teaching and support staff

1.2.6 Designated Safeguarding Lead (DSL)

1.2.7 Pupils

1.2.8 Parents / Carers

1.3 Acceptable Use Policies

1.4 Website and social media platforms

1.4.1 Email

1.4.2 Website

1.4.3 Digital Images

1.4.4 Social media / networking

1.5 Sanctions

1.5.1 Incidents of concern

1.5.2 Cyber Bullying

2. Infrastructure

2.1 Technical Security

2.2 Filtering

2.3 Personal Data

2.4 Personal Devices

2.5 Passwords

3. Education

3.1 Children

3.2 Staff

3.3 Governors

3.4 Parents and Carers

3.5 Equality Impact Assessment

4. Monitoring & Review

Appendix 1: Staff & Volunteer Acceptable Use Policy

Appendix 2: Pupil's Internet Code of Practice (EYFS)

Appendix 3: Pupil Acceptable Use Policy (KS1)

Appendix 4: Response to an incident of concern

Appendix 5: School E-Safety Incident Log

Appendix 6: E-Safety Audit

Appendix 7: Useful websites

1. Policy and Leadership

1.1 Scope

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

Keeping Children Safe in Education, September 2019. Annex C: Online safety

The development and expansion of the use of technology, and particularly the internet, has transformed learning in schools. Children need to develop high level ICT and Computing skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. Dropmore Infant School believes it is important to ensure that children are safe and protected from potential harm when using the internet and related communications technologies. In addition to implementing appropriate filtering and a monitoring system, recognising E-Safety issues and potential dangers and planning and educating accordingly should help ensure safe and appropriate use of communications technologies.

This E-Safety policy applies to all members of the school community who have access to and are users of the school ICT systems, both in and out of the school. Breaches of this E-Safety policy can lead to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that we are aware of the offline consequences that online actions can have.

1.2 Responsibilities

The school has appointed Mrs Gitta Streete as the E-Safety Coordinator to lead on E-Safety. She will work closely with the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL). The DSL and DDSL must be made aware of any disclosures, incidents or Child Protection concerns.

The E-Safety Policy relates to other policies including the Computing Policy, Child Protection Policy, Behaviour Policy, all subject policies and the School Improvement Plan.

1.2.1 Governors

The Governing Body will review the E-Safety policy and its implementation annually. They will take responsibility for revising the E-Safety policy and practice where necessary (such as after an incident or change in national legislation). Tim Wicks has been appointed to take lead responsibility for E-Safety within the Governing Body.

1.2.2 Headteacher

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community.
- The Headteacher and (at least) one other member of the Leadership Team 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).
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles.

1.2.3 E-Safety Coordinator (Mrs G Streete)

The E-Safety coordinator is responsible for:

- day to day monitoring of incidents and handling sensitive issues;
- developing and reviewing the school E-Safety policy;
- ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place;

- providing training and advice for staff;
- ensuring the technical support company (TurnITon) carries out all E-Safety measures;
- ensuring the technical support company (TurnITon) is fully aware of the school's E-Safety policy and procedures;
- meeting with E-Safety Governor;
- attending relevant Governor meetings;
- reporting to the Leadership Team.

1.2.4 Network Manager (TurnITon)

Dropmore has a managed ICT service provided by an outside contractor (TurnITon). The Network Manager is responsible for ensuring:

- ◆ that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- ◆ that the school meets required E-Safety technical requirements;
- ◆ that users may only access the networks and devices through an appropriate password protection policy;
- ◆ the filtering policy is applied and updated on a regular basis;
- ◆ anti-virus software is up-to-date;
- ◆ that 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;
- ◆ attempted misuse is reported to the Headteacher and E-Safety Coordinator for investigation.

1.2.5 Teaching and Support Staff

- have an up to date awareness of the current school E-Safety policy and practices;
- have read, understood and signed the Staff Acceptable Use Policy (AUP);
- report any suspected misuse or problem to the E-Safety Coordinator for investigation;
- ensure all digital communications with students / parents / carers should be on a professional level;
- ensure E-Safety is embedded in all aspects of the curriculum;
- ensure pupils understand and follow the E-Safety rules;
- monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities and implement current policies with regard to these devices;
- ensure processes are in place for dealing with any unsuitable material that is found in internet searches in lessons.

1.2.6 Designated Safeguarding Lead (DSL) & Deputy Designated Safeguarding Lead (DDSL)

The DSL and DDSL should be trained in and aware of the online safety issues. The potential child protection and safeguarding issues related to online safety can be classified into 3 areas of risk:

- ◆ content: being exposed to illegal, inappropriate or harmful material;
- ◆ contact: being subjected to harmful online interaction with other users;
- ◆ conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Keeping Children Safe in Education, September 2018. Annex C: Online safety

1.2.7 Pupils

- are responsible for using the school digital technology systems in accordance with the Pupils Acceptable Use Policy;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should understand procedures on the taking / using of images and on cyber-bullying;
- should understand the importance of adopting good E-Safety practice when using digital technologies.

1.2.8 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 take every opportunity to help parents understand these issues through parents' workshops, newsletters, assemblies, surveys and website information about E-Safety campaigns. Parents and carers will be encouraged to support the school in

promoting good E-Safety practice. They will be required to follow guidelines on the appropriate use of digital and video images taken at school events (see Chapter 1.4.3 Digital images). We believe that educational visits are an integral part of the entitlement of every pupil to an effective and balanced curriculum. Appropriately planned visits are known to enhance learning and improve attainment, and so form a key part of what makes Dropmore Infant School a supportive and effective learning environment.

1.3 Acceptable Use Policies

All staff must read and sign the Staff & Volunteer Acceptable Use Policy, before using any technology and annually thereafter (Appendix 1).

Parents must read the Pupil's Internet Code of Practice (Appendix 2) with their child and sign it, before their child is allowed to use any technology, when joining the school. The Pupil AUP (Appendix 3) will be shared and discussed during Computing curriculum time, at the start of every academic year in KS1.

All visitors to the school site who require access to the school network and/or internet will be asked to read and sign the Staff & Volunteer Acceptable Use Policy (Appendix 1).

1.4 Website and Social Media Platforms

1.4.1 Email

- We reserve the right to monitor all school email.
- The standard format for staff email accounts is smithj9@dropmore.bucks.sch.uk which can be accessed via gmail.
- Access in school to external personal email accounts may be blocked.

1.4.2 Website / Social Media

- ♦ The contact details on the website include the school address, email and telephone number. Staff or pupils' personal information is not published.
- ♦ The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- ♦ If an image of a child is used, the child's name will not be published. If a name is published, no image will be used without specific consent.
- ♦ Pupils' full names will not be used anywhere on the website.
- ♦ Only appropriate images and images considered safe from misuse will be used. Image file names will avoid using children's names.

1.4.3 Digital Images

- Images of a pupil will not be published without the parent's or carer's written permission. We ask permission to publish images of work or appropriate personal photographs once a year. Parents can withdraw their consent at any time by writing to the school.
- Parents and carers can use photographs and videos taken at school events for their own personal use only. Such photos and images must not be sold and must not be put on the web/ internet / social media. This applies to all forms of publications, including but not limited to print, film, video, DVD, websites and social media, and regardless of the device used.
- If parents and carers want to share a photograph or video, consent is required of all the other parents whose children are included in the images.
- We will remind parents / carers at the start of a school event that any images must be taken for personal use only. They will be reminded that such images must not be sold or put on the web / internet / social media.
- People with no connection to our school will not be allowed to take images – staff will question anyone they do not recognise.
- Staff and volunteers are not permitted to use their own personal devices to record pupil images.

1.4.4 Social Media/Networking

- Within the school environment access to social media and social networking sites will be part of filtering.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community will be advised not to publish specific and detailed private thoughts, especially those that may be considered confidential, sensitive, threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.
- Safe and professional behaviour will be outlined in the school Code of Conduct and the Staff (& Volunteer) Acceptable Use Policy (Appendix 1).

1.5 Sanctions

The school will take all reasonable precautions to ensure that children's exposure to online safety risks is limited. As part of this process appropriate filtering has been implemented (provided by EXA, see chapter 2.2) and a monitoring system is in place (see chapter 4).

1.5.1 Incidents of concern

- ♦ The school will manage any incidents by using the 'Response to an Incident of Concern' flowchart (Appendix 4)
- ♦ All members of the school community will be aware of the procedure for reporting E-Safety concerns (such as breaches of filtering, cyber bullying, illegal content)
- ♦ The E-Safety Coordinator will record all reported incidents and actions taken in the School E-Safety incident log (Appendix 5)
- ♦ The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately
- ♦ The school will manage E-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate
- ♦ The school will inform parents/carers of any incidents of concern as and when required
- ♦ After any investigations are completed, the school will debrief, identify lessons learnt, document and implement any changes required
- ♦ Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Bucks Safeguarding Children Board or the Police
- ♦ If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the County E-Safety Officer (acwatts@buckscc.gov.uk)
- ♦ If an incident of concern needs to be passed beyond the school then the concern will be escalated to the County E-Safety Officer to communicate to other school in Bucks.

1.5.2 Cyber Bullying

Cyber bullying or online bullying can be defined as "The use of technologies by an individual or by a group of people to deliberately and repeatedly hurt or upset someone else."

(<https://www.childnet.com/resources/cyberbullying-guidance-for-schools>)

- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Anti-Bullying Policy.
- All incidents of cyber bullying reported to the school will be recorded.
- Any incidents or allegations of Cyber bullying will be investigated by following the 'Response to an incident or concern' flowchart (Appendix 4).
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's E-Safety ethos.
- The school will take steps to investigate the incident and take appropriate action. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- The Police will be contacted if a criminal offence is suspected.
- Sanctions for those involved in cyber bullying may include:
 - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
 - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's Behaviour policy or Acceptable Use Policy.
 - Parent/carers of pupils will be informed.

2. Infrastructure

2.1 Technical Security

Dropmore Infant School has a managed ICT service provided by TurnITon. It is the responsibility of the E-Safety coordinator, to ensure that the managed service provider carries out all the E-Safety measures and is fully aware of the school E-Safety Policy and Acceptable Use Agreements.

- There will be regular reviews and audits of the safety and security of school technical systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, cabling, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users have clearly defined access rights to school technical systems and devices.
- The IT Co-ordinator will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The IT Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- An appropriate system is in place for users to report any technical incident / security breach to the ICT service provider, by using their community portal <https://uni.turniton.co.uk/>
- An agreed procedure is in place for the provision of temporary access of "guests" or "supply" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Workstations are secured against user mistakes.
- The server operating system is secure and kept up to date.
- Virus protection for the whole network is installed and current
- Access by wireless devices is secured with a minimum of WPA2 encryption
- The security of the school information systems will be reviewed at least annually.
- SPI should not be kept on personal computers, laptops or mobile devices.
- Portable media and unapproved software may not be downloaded or used without specific permission from the IT Co-ordinator or network manager.
- The school reserves the right to check any files held on the school's network.
- The network manager will review system capacity regularly.

2.2 Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for E-Safety and acceptable use.

- ◆ The responsibility for the management of the school's filtering policy is held by TurnITon. They will manage the school filtering, in line with this policy and will keep logs of changes to and breaches of the filtering systems
- ◆ To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to the E-Safety coordinator
- ◆ All users have a responsibility to report immediately to the E-Safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered
- ◆ Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials
- ◆ Internet access is filtered for all users by the school's ISP (EXA). It includes quantum SSL filtering which is fully compliant with KCSiE 2019.
- ◆ Illegal content is filtered by EXA. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.
- ◆ In the event of staff needing to switch off the filtering for any reason, or for any user, this must be agreed by the Headteacher or E-Safety Coordinator
- ◆ Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- ◆ Any filtering issues should be reported immediately to the filtering provider by the E-Safety coordinator.

2.3 Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 (GDPR).

Please see the school's Data Protection Policy for more information.

2.4 Personal Devices

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices will not be used in school during lessons, extra-curricular activities or school events, unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile phones and devices will be switched off or switched to 'silent' during teaching periods.
- Bluetooth communication should not be used unless it is part of an educational activity and approved by the Senior Leadership Team.
- Mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

2.5 Passwords

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager.
- The “administrator” passwords for the school systems, used by the technical staff must also be available to the Headteacher and members of the senior Leadership team.
- Passwords for new users, and replacement passwords for existing users will be allocated by the IT Co-ordinator.
- All users (adults and children) will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Staff passwords

- ◆ All staff users will be provided with a username and password by the IT coordinator who will keep an up to date record of users and their usernames.
- ◆ Staff passwords should be a minimum of 8 characters long and must include three of: uppercase character, lowercase character, number and special characters.
- ◆ Staff passwords must not include proper names or any other personal information about the user that might be known by others.
- ◆ The account will be “locked out” following six successive incorrect log-on attempts.
- ◆ Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- ◆ Passwords shall not be displayed on screen, and shall be securely hashed (one-way encryption)
- ◆ Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised.
- ◆ Passwords should be changed annually.
- ◆ Staff should not re-use passwords. They should be significantly different from previous passwords.

Student passwords

- All users will be provided with a username by the IT coordinator who will keep an up to date record of users and their usernames.
- Student passwords will be changed at the start of every school year, with increased complexity as they move through the school.
- Students will be taught the importance of password security.
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

3. Education

3.1 Children

- An E-Safety module forms part of the Computing scheme of work for each class, to raise the awareness and importance of safe and responsible internet use amongst pupils both at school and at home.
- E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum.
- Key E-Safety messages are reinforced as part of a planned programme of assemblies and pastoral activities.
- E-Safety posters and copies of the Pupil Acceptable Use Policy will be posted in all classrooms.
- 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.
- Pupils will be guided to use age-appropriate tools to research Internet content.
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils’ age and ability.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.
- Staff should act as good role models in the use of digital technologies, the internet and mobile devices.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites they visit.

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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. Useful e-Safety programmes include:

- Safer Internet Day: <https://www.saferinternet.org.uk/>
- Think U Know: www.thinkuknow.co.uk
- Childnet: <https://www.childnet.com/>

3.2 Staff

- ♦ The E-Safety Policy, Acceptable Use Policies and 'Response to an incident of concern' flowchart have been formally shared and discussed with all members of staff and will be reviewed annually thereafter.
- ♦ Induction of new staff will include a discussion about the school E-Safety Policy, the Acceptable Use Policies and the 'Response to an incident of concern' flowchart.
- ♦ Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- ♦ Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, is on-going for all members of staff.
- ♦ All members of staff are aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- ♦ The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- ♦ This E-Safety policy and its updates will be presented to and discussed by staff in meetings/INSET days
- ♦ The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

3.3 Governors

Governors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any committee involved in technology / E-Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisations.
- Access to training sessions for staff/parents.

3.4 Parents and Carers

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to E-Safety at home and at school with parents will be encouraged. This includes offering regular parent forums, courses, awareness sessions or highlighting e-Safety at other attended events e.g. parent evenings.
- When joining the school, parents will be requested to read the Pupils' Internet Code of Practice (Appendix 2), discuss it with their child, and sign it.
- At the start of Year 1 and Year 2, parents will be requested to read the Pupil Acceptable Use Policy (Appendix 3), discuss it with their child and sign it.

- E-Safety contacts and resources, including websites with advice on filtering systems and responsible use of the Internet and educational and leisure activities will be made available to parents (App. 7).

Parents and Carers play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children 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:

- ◆ E-Safety workshops
- ◆ Letters, newsletters, website
- ◆ Safer Internet Day
- ◆ Reference to the relevant web sites / publications (Appendix 7)

3.5 Equality Impact Assessment

This policy has been written with reference to and in consideration of the school's Equality and Cohesion Policy. At Dropmore Infant School we promote equality and diversity, challenge discrimination and celebrate diversity. We ensure that everyone is treated fairly, with dignity and respect; irrespective of race, gender, disability, pregnancy and maternity, age, sexual orientation, gender identity and religion/belief. We provide opportunities accessible to all; and ensure that the needs, entitlements and outcomes for all pupils, staff and parents are met.

4. Monitoring and Review

Monitoring of E-Safety incidents takes place and incidents are recorded on the E-Safety incident log.

The school will complete an E-Safety audit annually to establish if the e-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate (Appendix 6).

The E-Safety Policy will be reviewed annually, or more regularly in the light of any new significant new developments if the use of the technologies, new threats to E-Safety or incidents that have taken place



APPENDIX 1: Dropmore Infant School Staff (& Volunteer) Acceptable Use Policy



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.

SECURITY & PRIVACY:

- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will use a 'strong' password. A strong password has 8 or more characters and must include three of uppercase character, lowercase character, number and special characters.
- To prevent unauthorized access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will immediately report any illegal, inappropriate or harmful material to the E-Safety Coordinator.
- I will not try to use any programmes or software or alter settings that might allow me to bypass the filtering or security systems in place.
- I will not download, upload or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not keep professional documents which contain school-related sensitive personal information on any personal device and will only use school provided devices that are secure and encrypted.
- I will not use a personal camera or camera phone to record pupil images.
- I will not publish any images of pupils outside the school environment without express permission from the parents and the Head teacher.
- If offensive materials are found, I will immediately switch off the monitor, cover the computer, confiscate any printed materials and report it to the E-Safety coordinator.
- I have read and understood the E-Safety policy which covers the requirements for safe ICT use.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the E-Safety Coordinator.

(EMAIL / INTERNET) COMMUNICATION:

- I will access the internet for educational purposes only.
- I will communicate in a professional manner; I will not use aggressive or inappropriate language.
- I will only communicate with pupils, parents/carers and other professionals via the approved communication channels.
- I will only respond to messages received from children relating to school matters.
- I will not open any attachments to emails, unless the source is known and trusted
- I will not use personal email addresses on the school ICT systems.
- I will ensure that I have permission to use the original work of others in my work.
- Where work is protected by copyright, I will not download or distribute copies (incl. music and videos).
- I understand that disciplinary action may be taken if the internet is used inappropriately.

EQUIPMENT:

- I understand that the rules set out in this agreement also apply to use of school equipment and systems out of school (e.g. laptops, email).
- I will only use the school ICT systems for professional and educational purposes.
- When using portable media I will ensure they have been checked by anti-virus software and are free from viruses.
- I will not access, copy, remove or alter any other user's file, without prior permission.
- I will not download or install software from the internet or attached to emails without permission.
- I will protect computer equipment from spillage by eating and drinking well away from them.
- I will leave my personal mobile devices in a locker or the school office during school hours.



Dropmore Infant School
Staff (& Volunteer) Acceptable Use Agreement Form



This form relates to the Dropmore Infant School Staff (& Volunteer) Acceptable Use Policy (AUP), to which it is attached. Please read this document carefully and complete the sections below to show that you have read and understood the AUP.

I understand that if I fail to comply with this Acceptable Use Policy I could be subject to disciplinary action.

I have read and understood 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:

/


Signature:

Date:
DD/MM/YYYY



APPENDIX 2:
Dropmore Infant School
Pupils' Internet Code of Practice (EYFS)



	<p style="margin: 0;">Dropmore Infant School</p> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> <p style="margin: 0;"><i>Pupils' Internet Code of Practice</i></p>
<p><i>My Internet Promise</i></p> <ul style="list-style-type: none">• I will only use the Internet when a teacher or adult is with me.• I will never type in my personal information <u>OR</u> that of others (i.e. home address or telephone number, school name and address) unless my teacher specifically gives me permission.• I will never send anyone my picture without permission from my teacher.• I will never give my password to anyone; even my best friend.• I will log off when I have finished using the computer or laptop.• I will always be myself and will not pretend to be anyone or anything I am not.• I will look after all equipment. <p>✂ _____</p> <p style="text-align: center;"><u>Pupils' Internet Code of Practice</u></p> <p>Pupil's Name: Year:</p> <p>I have read the Pupils' Code of Practice and I have discussed it with my son/daughter. I agree to support the school's policy on the use of the Internet.</p> <p>Signed (Parent/Guardian): Pupil:</p> <p>Date:</p>	



APPENDIX 3: Dropmore Infant School Pupil Acceptable Use Policy (KS1)



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.

INTERNET:

- I will only use the internet when a teacher or adult is with me.
- I understand that the school knows which web sites I visit.
- I understand that I can only access sites for my work in school.
- I know that information on the internet may not always be true.
- I know that I will not be allowed to use the internet if I look at unsuitable material on purpose.

SECURITY & PRIVACY:

- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher or parent/carer.
- I will never give my password to anyone, even my best friend.
- I will never arrange to meet anyone in person without first agreeing it with my teacher or parent/carer and I will get them to come along to the first meeting.
- I will never respond to any worrying or unkind emails or messages. I will tell my teacher or parent/carer straight away.
- I will not look for bad words or pictures while I am online. I will tell my teacher or parent/carer straight away if I see any.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I will not take or share images of anyone without their permission, not even my friends.
- I respect other people's work and will not access, copy, remove or change any other user's files.
- I will be polite and responsible when I communicate with others
- I will only use kind language.

EQUIPMENT:

- I will log off when I have finished using the computer.
- I may not use removable media (CD, Flash drive, memory sticks etc.) brought in from home unless I have asked my teacher.
- I will not eat or drink near computer equipment.
- I will look after all computer equipment and will report any damage straight away.



Dropmore Infant School Pupil Acceptable Use Agreement Form



This form relates to the Dropmore Infant School Pupil Acceptable Use Policy (AUP), to which it is attached. Please read this document carefully and complete the sections below to show that you have read and understood the AUP, discussed it with your child and agree to the rules included.

If any pupil does not comply with this Acceptable Use Policy (AUP), access to the school ICT systems will be suspended and the student will be subject to disciplinary action. Additional action may be taken in line with the school's Behaviour and Discipline Policy. For serious violations, suspension or expulsion may be imposed. Where appropriate, the police may be involved or other legal action taken. For more information please see the schools E-Safety Policy.

Only once this agreement form has been signed and returned will access to the school ICT systems be permitted.

I have read and understood the above and agree to follow these guidelines when:

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

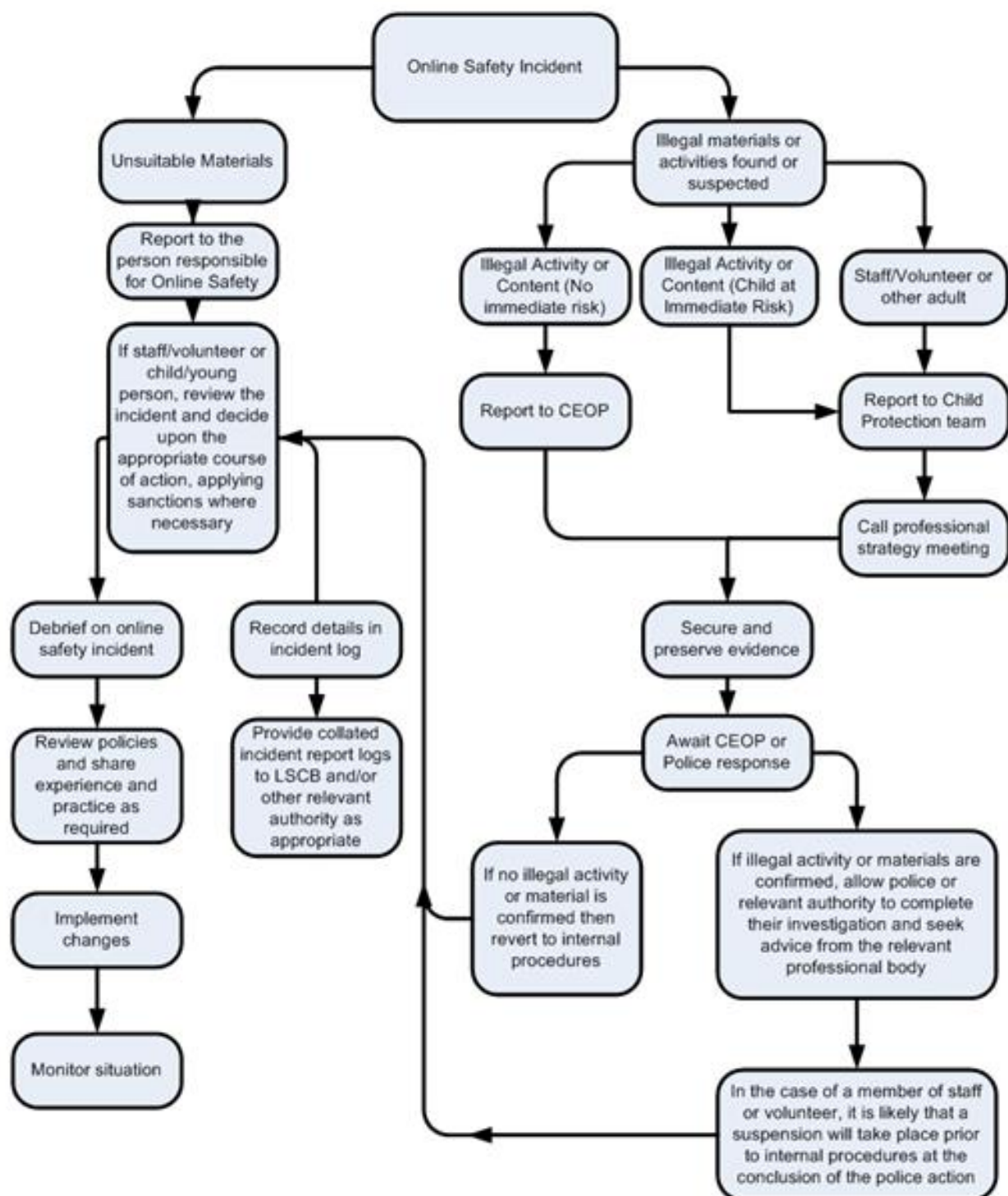
Name of Pupil:

Parent/Carer
Name:

Parent/Carer
Signature:

Date:
DD/MM/YYYY

APPENDIX 4: Response to an Incident of Concern



LSCB = Local Safeguarding Children Board
CEOP = Child Exploitation and Online Protection

APPENDIX 5: Dropmore Infant School Incident Log



Dropmore Infant School e-Safety Incident Log



Date & Time	Name of pupil or staff member	Room & computer/device n.r.	Details of incident	Actions & Reasons

APPENDIX 7: Useful Websites

Buckinghamshire Local Safeguarding Children Board:

<https://www.bucksscp.org.uk/professionals/e-learning/>

CEOP: <https://www.ceop.police.uk/safety-centre/>

Childline: www.childline.org.uk

Childnet: <https://www.childnet.com/>

Connect Safe – Parents Guide to Facebook: <http://www.connectsafely.org/facebook-for-parents/>

Cyberbullying: <http://www.cyberbullying.org/>

Digizen: www.digizen.org.uk

Get Safe Online: <https://www.getsafeonline.org/safeguarding-children/>

Internet Watch Foundation (IWF): <https://www.iwf.org.uk/> (copy and paste link)

Netsmartz: <http://origin.www.netsmartz.org/Home>

NSPCC: <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

Respectme: <http://www.respectme.org.uk/>

Safer Internet Centre: <https://www.saferinternet.org.uk/>

SWGfL: <https://swgfl.org.uk/online-safety/>

Thames Valley Police: <http://www.thamesvalley.police.uk/>

Think U Know website: www.thinkuknow.co.uk

UKCCIS UK Council for Child Internet Safety:

<https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

<https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis>

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

360safe safety self-review: <https://www.360safe.org.uk/>