DUKE of KENT
SCHOOL

7h - E-Safety Policy

November 2021

Duke of Kent School, Peaslake Road, Ewhurst, Surrey GU6 7NS
Tel: 01483 277313 Email: office@dokschool.org

1. Aims

Aims:

The Head and Governors of Duke of Kent School recognise the importance of e-learning and the significant benefits presented to pupils, staff and parents by the emerging technologies used at home, at School and in the workplace. There are also significant risks inherent in the use of these technologies and this policy aims to minimise these risks by:

- ensuring that all with responsibilities in the area of e-safety clearly understand their roles and duties
- explaining the School's approach to e-safety
- providing a framework for the handling of e-safety incidents

This policy should be read in conjunction with other School policies, particularly the Anti-Bullying Policy, Acceptable Use policies, Behaviour Policy, Staff Code of Conduct and Safeguarding Policy.

Duke of Kent School recognise that the use of technology has become a significant component of many safeguarding issues such as: Child Sexual Exploitation, Radicalisation, Sexual Predation and others. Duke of Kent School educates staff, students and parents to help reduce the risk of harm online by focusing on the four categorised areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

2. Responsibilities

The Chair of Governors:

is responsible for appointing a Safeguarding Governor, with lead responsibility for e-safety, who will:

- review this policy at least annually and as necessary in response to any e-safety incident to ensure that the policy is up to date and covers all aspects of technology use within the school.
- keep up to date with emerging risks and threats through technology use
- receive termly updates from the Head in regards to training, identified risks and any incidents
- keep the Chair of Governors and fellow Governors updated on e-safety matters
- attend the E-Safety Committee where possible
- provide the Head, Head of Safeguarding and E-Safety Co-ordinator advice on matters connected with e-safety
- with the E-Safety Co-ordinator undertake an annual review of how e-safety incidents have been dealt with and ensure the policy was effective and appropriately applied in managing those incidents

Head and E-Safety Co-ordinator

The Head has overall responsibility for e-safety within the School and will appoint an E-Safety Co-ordinator. Necessary resources for e-safety will be allocated by the Head. The E-Safety Co-ordinator will:

- keep up to date with emerging risks and threats through technology use

- undertake CEOP training as necessary
- have appropriate training and professional development in order to undertake the role
- ensure that all e-safety incidents are dealt with promptly and appropriately
- advise the Head, Governors and staff on all e-safety matters
- co-ordinate responses to e-safety incidents, in consultation with relevant Heads of Section; where Safeguarding issues are involved, the Head of Safeguarding must also be alerted and Safeguarding procedures will be followed
- ensure e-safety training throughout the school is planned and up to date and appropriate to the recipient: pupils, staff, senior leadership team and governing body, parents
- keep up to date with the latest risks to children whilst using technology and with the latest research and available resources for school and home use, undertaking any necessary training
- keep up to date with the latest PREVENT advice linked to online safety
- engage with parents and the School community on e-safety matters at School and at home
- liaise with Surrey Safeguarding e-safety team, IT technical support and other agencies as required
- retain responsibility for the e-safety incident log; ensure staff know what to report and how to document concerns or incidents
- attend the Governors' IT committee (termly strategic group) to represent and report on e-safety issues
- review this policy regularly and bring any matters of concern to the attention of the Head
- with the Safeguarding Governor undertake an annual review of how e-safety incidents have been dealt with and ensure the policy was effective and appropriately applied in managing those incidents
- brief the Head on e-safety incidents and concerns including recommending any necessary changes to policy or practice
- review reports of flagged searches on the network provided by the Network Manager

Network Manager

The Network Manager is responsible for ensuring that:

- the IT technical infrastructure is secure
- anti-virus is fit-for-purpose, up to date and applied to all capable devices
- operating systems updates are regularly monitored and essential updates applied
- e-safety technical solutions such as Internet filtering / iPad central control systems / Chromebook management are operating correctly and safely
- filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety Co-ordinator and Head
- passwords are applied correctly to all users regardless of age
- the Network Manager and his team keep up to date with the latest risks to children whilst using technology, undertaking any necessary training
- on the request of the E-Safety Co-ordinator or Head or with their own reasonable suspicions, review and report on individual user activity on the network or School provided devices
- the Head and E-Safety Co-ordinator are alerted as a matter of urgency to any vulnerability, security breach, attack or incident known to have caused or likely to have caused (including 'near misses') an e-safety risk to pupils or staff
- advice is provided to parents who have technical questions about e-safety, on request of the E-Safety Co-ordinator
- advice on technical matters of e-safety is provided to staff when required
- IT System Administrator security is in place (to include the regular changing of administrator passwords)
- patterns of pupil and staff use of the network are regularly monitored; the Network Manager will ensure that any unusual or potentially dangerous uses or incidents are brought swiftly to the attention of the E-Safety Co-ordinator; where Safeguarding issues are involved, the Head of Safeguarding must also be alerted
- any issues related to data protection are referred to the Operations Bursar
- provide flagged search updates to the e-safety co-coordinator and assist in tracking

All Staff

All teaching and classroom support staff are users of the network and have signed Acceptable Use policies which must be followed. They are also responsible for ensuring that:

- they understand all details within this policy. If anything is not understood it should be brought to the attention of the Head or E-Safety Co-ordinator
- they understand what cyber-bullying is and respond according to the Anti-Bullying Policy
- any e-safety incident is reported as quickly as possible to the E-Safety Co-ordinator(who may also refer the reporting member of staff to the Head of Safeguarding), or in their absence to a member of the Safeguarding Team. Staff who are unsure of whether an incident should be reported should raise the matter with the E-Safety Co-ordinator
- they seek any support, training or advice they require in this rapidly changing area from the E-Safety Co-ordinator
- they report any copyright or plagiarism issues to the Head
- they follow the guidelines outlined in the Staff Social Media Policy related sections in the Staff Handbook. Staff are reminded that e-safety incidents often involve Safeguarding issues; School Safeguarding procedures must be followed.

All Pupils

Pupils are responsible for their behaviour on the network and devices provided by the School just as they are in a classroom, the corridor or games pitch. In order to use the network and devices provided by the School, pupils sign Acceptable Use Policies (See Appendices) and these must be followed. The boundaries of use of ICT equipment and services for pupils at Duke of Kent School are given in the Student Acceptable Use Policy; breaking these rules or misusing ICT equipment or services will be dealt with in accordance with the Behaviour Policy. Sanctions may include temporary or permanent exclusion, at the discretion of the Head.

Cyber-bullying is any form of bullying which takes place online or through smartphones and tablets. Social networking sites, messaging apps, gaming sites and chat rooms such as Facebook, XBox Live, Instagram, YouTube, Snapchat and other chat rooms. (bullying.com 2021)

Pupils should:

- understand what cyber-bullying is
- understand that the School will not tolerate cyber-bullying and that pupils who cyber-bully, particularly when this is repeated or aggressive in nature, can expect to be suspended or expelled from School
- understand that being a 'bystander' or passing on images or messages created by cyber- bullies could itself be defined as cyber-bullying
- be aware that if investigation of an e-safety incident suggests that a pupil's misbehaviour may be criminal or pose a serious threat to a member of the public, the Head will contact the Police

When pupils have a concern or a question about how others are treating them / how a friend or another pupil is being treated / their own behaviour they are expected to bring this promptly to the attention of a teacher or parent so that help, support and advice can be provided.

Parents and Carers

The School recognises that emerging technologies present significant challenges to parents who often have questions or concerns about e-safety and the School will aim, through parents' evenings, bulletins and other communicatoins and briefings from the E-Safety Committee, to keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Duke of Kent School strongly recommends that parents follow the advice provided by CEOP (Child Exploitation Online Protection) via the website www.thinkuknow.co.uk as this provides regularly updated information for parents of children of all ages and useful age-appropriate material to look at together with your children.

Through assemblies, form periods, subject lessons and the PSHE programme, e-safety is both taught discretely and embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff and made aware of how they can report areas of concern whilst at School or outside of School. Parents should be aware that evidence of cyber-bullying taking place outside of School may result in School sanctions, up to and including expulsion, according to the rules set out in the Behaviour Policy.

Duke of Kent School takes a proactive approach to e-safety. Parents should note however that many areas including:

- the number of hours children spend on the internet or using mobile devices at home
- the hours during which children are permitted access to the internet or mobile devices at home
- the types of interaction on the internet permitted (e.g. unregulated contact with peers, contact with strangers) at home
- the security settings and permissions on home equipment and devices
- adherence to gaming/video/social networking age guidelines, regulations and laws
- permission to join social networking sites or online gaming or chat

are parenting decisions in which the School can provide advice but over which the School ultimately has no control. It is absolutely essential, therefore, that parents exercise vigilance and take responsibility for these vital aspects of modern family life.

Parents are responsible for:

- bringing swiftly to the attention of the E-Safety Co-ordinator or Head of Safeguarding any e-safety concerns
- concerns over cyber-bullying or inappropriate uses of digital technology
- ensuring that School devices are used appropriately at home, adhering to the e-safety policy and School AUPs, by students and other members of the household

Parents are reminded that, as in all parenting matters, values and practices vary significantly from family to family. When their children visit friends' homes, parents are advised to discuss in advance with the friends' parents their expectations for access to and use of technology (e.g. mobile phone access, gaming, internet use, film age ratings).

Where minor difficulties arise between children of families known to each other in the offline world, parents can often deal with these by sensitive contact with the parents of the child concerned. It will be helpful to keep the School informed of any relevant information. In the event that this approach is not possible or desirable, parents can seek advice from the E-Safety Co-ordinator or School Child Protection Officer. In a serious case which might involve criminal offence or risk to an individual, parents or the School may need to contact agencies such as CEOP (via their website) or the Police: when a child is in immediate danger, 999 should be called.

Parents with concerns, questions or suggestions regarding e-safety are encouraged to contact the E-Safety Co-ordinator who will be happy to discuss these and to provide advice. Parents and staff are advised that they must not forward to the School digital material (e.g. an offensive image sent to their child) which they believe to be offensive or criminal in nature as this action may in itself constitute a criminal offence.

3. E-Safety Committee

Chaired by the E-Safety Co-ordinator, the E-Safety Committee is responsible for:

- advising on changes to the e-safety policy
- monitoring the effectiveness of e-safety training and awareness in the School

- recommending further initiatives for e-safety training and awareness at the School

Comprising volunteer pupils, parents, E-Safety Co-ordinator and others as required, the E-Safety Committee will commence twice each academic year.

4. Internet Access at Duke of Kent School

Access to technology at School is considered a privilege and not a right. Pupils and staff are responsible for their behaviour in the online world just as in a corridor, in a classroom or on a pitch.

- All staff must read and sign the 'Staff Acceptable Use Policy for ICT' before using any School ICT resource.
- The School will maintain a current record of all staff and pupils who are granted access to School ICT systems, Chromebooks and iPads.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- All pupils must read and sign the 'Pupil Acceptable Use Policy for ICT' before using any School ICT resource.
- Any person not directly employed by the School will be asked to sign an acceptable use policy before being allowed to access the internet from the School site.

5. Teaching of Internet Safety

The teaching of e-safety is embedded throughout the curriculum across the age ranges of the School. Students study a program of PSHE from Reception to Year 11 and e-safety sessions are planned within those schemes.

In the Pre-Prep and Prep School sessions are delivered through the weekly PSHE lessons and they are planned based on the requirements and needs of the year groups. For example Year 6 have more sessions than Year 3 due to an increased presence online at that age. These sessions are complemented by regular talks from the e-safety coordinator and any other relevant speakers.

In the Senior School sessions are again planned into the PSHE curriculum; lessons are delivered weekly by form staff. Many of the sessions throughout the year link with the many of the themes of e-safety, and there is a particular focus on e-safety during Spring Term 1.

The sessions and planning is informed by the UKCCIS 'Education for a Connected World'[1] document and the PHSE Schemes of Work planned by the PHSE Co-Ordinator. This enables lessons to be tailored to the year groups.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF

6. Misuse of Technology

The following table outlines some of the ways technology can be misused and the acceptability of the behaviors at Duke of Kent School:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the School or brings the School into disrepute				X	
Using School systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media				X	
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

The actions and sanctions for the misuse of technology can be found in the appendix.

7. How E-safety Incidents are Reported and Dealt With

E-Safety Incidents are dealt with in conjunction with Duke of Kent School's behavior policy.

Concerns regarding e-safety will be dealt with initially by the e-safety coordinator. Any concern or complaint about internet misuse by the staff must be referred to the Head. Concerns which involve Safeguarding must be dealt with in accordance with School Safeguarding procedures.

Duke of Kent School will ensure that pupils, parents and staff are informed annually, via the Behaviour Policy, of the consequences and sanctions for misuse of the internet and emerging technologies.

Following the report of an e-safety incident, the E-Safety Co-ordinator will take action which may include:

- inviting relevant parties (this may include pupils, parents, staff) to discuss the incident, its impact, how it can be resolved and how repetition can be avoided
- providing e-safety advice
- briefing staff
- seeking external agency advice

Where cyber-bullying is deemed to have taken place, the Anti-Bullying policy will be followed. If investigation of an e-safety incident suggests that a pupil's misbehaviour may be criminal or pose a serious threat to a member of the public, the Police may be contacted, at the discretion of the Head.
A flow chart on the immediate response to e-safety incidents can be found in the appendix.

8. Managing Emerging and Mobile Technologies

- Emerging technologies will be examined for educational benefit and risks evaluated before use in School is allowed. The advice of the Governors' IT Committee may be sought.
- The School provides devices (iPads and Chromebooks) that are owned by School for students and staff. They are under the network restrictions of the School and their use should be in line with the AUPs that students and staff have signed. The School allocates the devices and responsible personal use is allowed outside of lessons.
- Mobile telephones are not permitted in School for pupils. If a pupil needs to bring a telephone for any reason (e.g. travel by bike or bus), it must be checked in and out of the School Office at the beginning and end of the day. Students who are found with a mobile phone in School will be set a Friday detention, if a repeat offence is recorded then an internal suspension will be issued.
- No device that can be used to access the internet, send texts or emails or store images is

permitted in School for pupils.

- Cameras and recording equipment must only be brought to School with a teacher's permission and must be stored according to the teacher's instructions. No image (still or moving) or audio recording taken in School or from any School activity must be posted on the internet without written permission from a member of staff.
- Staff will use a School phone whenever possible where contact with pupils or parents is required.

9. Protecting Personal Data and GDPR

Duke of Kent School takes the storage of personal data seriously and complies with GDPR legislation. For further information please see these School documents:

- Information and Records Retention Policy
- Privacy Notices for Staff / Younger Students / Older Students / Parents

that can be found here:

http://www.dukeofkentschool.org.uk/about-duke-of-kent/school-information-and-policies

The School use Google Education Suite and have completed the due diligence checks on cloud based storage of information.

10. EYFS Photos and Phones

Please see the School's Safeguarding for information on photos and phones in EYFS.

11. Filtering

The School will ensure systems to protect pupils are reviewed and improved and that the filtering methods selected are appropriate, effective and reasonable. If staff or pupils come across unsuitable on-line materials, the site must be reported to the e- safety Coordinator. A log of any incidents may be useful to identify patterns and behaviours of the pupils.

The school uses:

Upstream: Norton Familysafe DNS

In-house: 'Untangle' Granulated by age group to filter the content accessed on the School network.

The Schools' filtering system manages the following content:

- Illegal Online Content
- Discrimination
- Drugs / Substance abuse
- Extremism
- Malware / Hacking
- Pornography
- Piracy and Copyright Theft
- Self-Harm
- Violence

The filtering system meets the following principles:

- Age Appropriate filtering
- Control of the filter
- Identification of individual users

- Ability to block content on Apps
- Applied at network level
- Has a reporting mechanism
- Can report on historical information on the websites visited by users

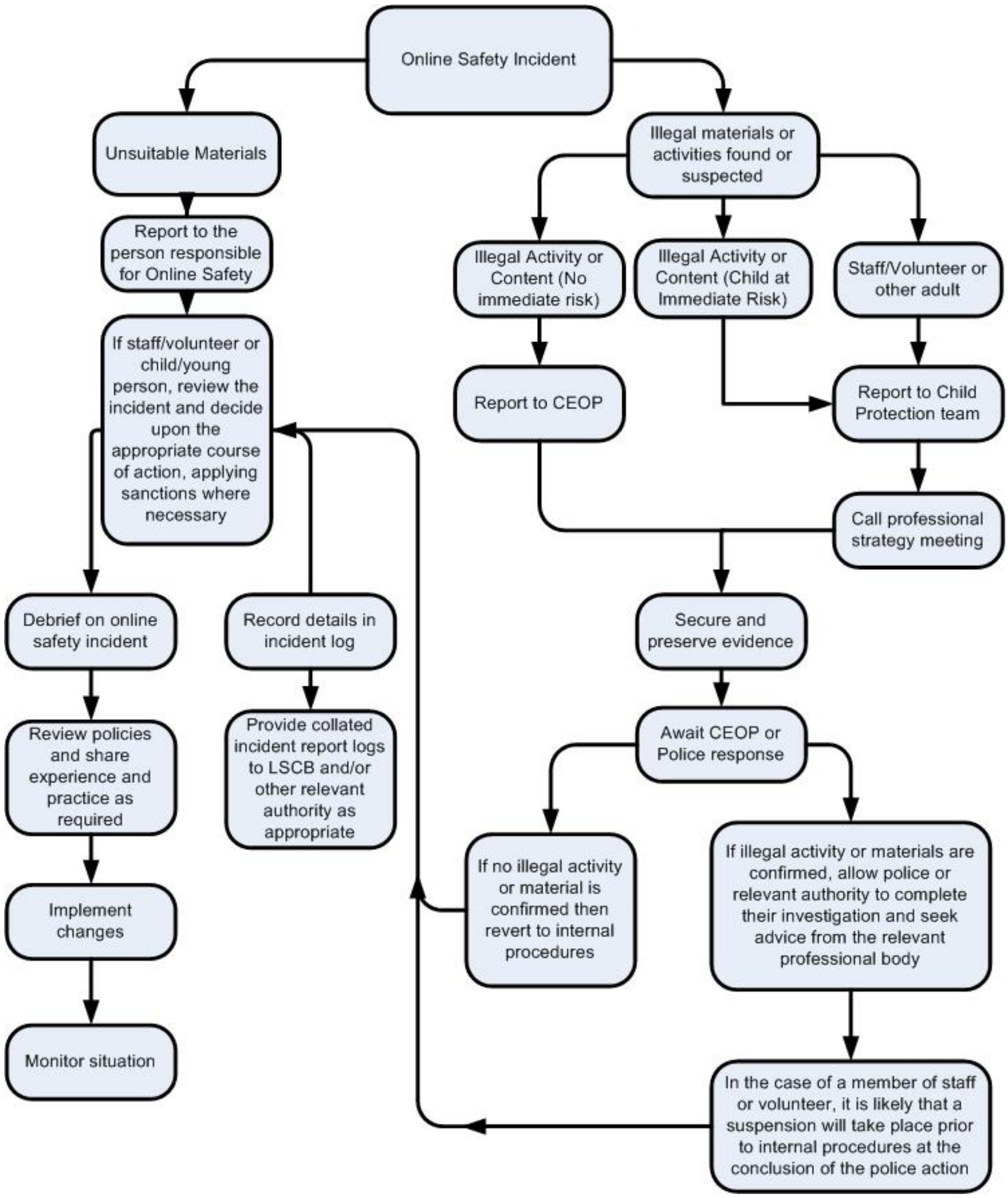
12. Staff Training and Student Sessions

Throughout the year there are many e-safety themed events and training for staff, students and parents. These include:

Staff	Students	Parents
All teaching staff complete 'Online Safety' module on Educare	All senior students will receive a talk on Online Safety and Ethics from Eagle Radio	A weekly tip in the School's bulletin
E-Safety updates on INSET days	Safer Internet Day celebrations across the School	Sessions throughout the year aimed at different age groups: PrePrep – Forum Prep School and Seniors- Talk / Presentations
Regular updates on developments in online safety	School Assembly updates	E-mailed up to date copies of 'Digital Parenting'
PREVENT training	PSHE program lessons.	
	Visiting speakers	

Person Responsible for this policy: E-Safety Co-ordinator
Reviewed: November 2021
Next Review: October 2022

Appendix 1 – Flow Chart for Incidents


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 2 – Actions and Sanctions

	Actions / Sanctions								
Students / Pupils Incidents	Refer to Head of Section	Refer to E-Safety Coordinator	Refer to Headteacher	Refer to Police	Refer to MASH	Inform parents / carers	E-Safety Education	Warning	Further sanction eg debit / stripe / suspension / Exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X			X
Unauthorised use of non-educational sites during lessons	X						X		
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X						X		X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X				X	X		X
Unauthorised downloading or uploading of files		X	X				X		X
Allowing others to access School network by sharing username and passwords		X					X		X
Attempting to access or accessing the School network, using another student's account		X	X				X		X
Attempting to access or accessing the School network, using the account of a member of staff		X	X			X	X		X
Corrupting or destroying the data of other users		X	X				X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X		X
Continued infringements of the above, following previous warnings or sanctions			X			X			X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			X			X			X
Using proxy sites or other means to subvert the School's filtering system		X	X			X	X		X

Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X			X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X					X		X

Appendix 3 – Extract of IT Use from Pupils Code of Conduct Policy

4. Rules for IT

i) You are responsible for your behaviour on the network and devices provided by the School just as you are in a classroom, the corridor or games pitch.
ii) Use of IT is a privilege and not a right. In order to use the network and devices provided by the School, you have signed an IT Acceptable Use policy and this must be followed. If you break it, this may mean you have no access to computers at School. Serious incidents could lead to suspension or expulsion. If you are not sure whether an activity is permitted, check with the Network Manager.
iii) Mobile telephones are not permitted in School for pupils. If you need to bring your telephone for any reason (e.g. travel by bike or bus), it must be checked in and out of the School Office at the beginning and end of your day.
iv) Cameras and recording equipment must only be brought to School with a teacher's permission, and must be stored according to the teacher's instructions. No image (still or moving) or audio recording taken in School or from any School activity must be posted on the internet without written permission from a member of staff.
v) No device that can be used to access the internet, send texts or emails or store images is permitted in School for pupils without the Head of Section's permission.
vi) If you have a 1-1 or shared DoK iPad, you must follow all the instructions given by your teachers regarding its use and storage, and you must keep to the iPad Acceptable Use Policy.
vii) You must not identify yourself as a member of the School on a social network site either directly or indirectly (e.g. photograph in school uniform, use of a school email). You must not make reference to the School, pupils or staff on the internet or social networks without written permission of a member of staff.
viii) Responsible behaviour online is expected, in and out of School. Serious sanctions will follow any attempt to humiliate, ridicule or intimidate others online. Sexting (sending naked or indecent images of yourself or others, or sending on such images if you receive them) is not acceptable and may result in serious sanctions and investigation by the Police.

It is important that you understand what cyber-bullying is:

Cyberbullying is using the internet, email, online games or any digital technology to threaten, tease, upset or humiliate someone else. (Childline 2016)

- The School will not tolerate cyber-bullying and pupils who cyber-bully, particularly when this is repeated or aggressive in nature, can expect to be suspended or expelled from School.
- Being a 'bystander' or passing on images or messages created by cyber-bullies could itself be
defined as cyber-bullying.
- If investigation of an e-safety incident suggests that a pupil's misbehaviour may be criminal or pose a serious threat to a member of the public, the Head may contact the Police.

When you have a concern or a question about

- how others are treating you in the cyber-world
- how a friend or another pupil is being treated online
- your own behaviour online

you are expected to bring this promptly to the attention of a teacher or parent so that help, support and advice can be provided. Failing to do so, is a breach of this Code.

Appendix 4 – Student AUP

Pupil Name:	**Year Group:**

DUKE OF KENT SCHOOL
Pupil ICT Acceptable Use Policy
For Years 4 and above

ICT and related technologies such as the internet and mobile devices are an expected part of our daily School life. This policy is designed to ensure that all pupils are aware of their responsibilities when using any form of ICT. All pupils are expected to adhere to the content of this Acceptable Use Policy at all times.

All Pupils are expected to read through and comply with the Pupil ICT Acceptable Use Policy. Failure to do so may result in the withdrawal of the use of all ICT.

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 on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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 alter 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 and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have 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 validity of 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 access social media sites on school devices unless permission to do so has been given.
- I will respect school devices and ensure they are not damaged, defaced and treated with respect.

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.
- Access to the internet and use of devices outside of lesson time should only be done with the permission of a teacher.
- 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.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police. Information on actions and their consequences can be found in the e-safety policy.

Pupil Signature. ………………………………………………………Date……………………………..

Appendix 5 – Chromebook Agreement

Senior School: Chromebook Agreement 2021

The Chromebooks are a device provided to you by the school to aid your learning. They are to be used to enhance and support your education. As a school, we have a right to remove the device from you should you not adhere to the agreements set out below, the Network AUP (Acceptable Use Policy) that you have signed, or the E-Safety Policy (found on the school website).

The following points relate to your use and treatment of the Chromebooks and must be followed both in school and at home:

1. The Chromebook should only be used for educational purposes. They should **NOT** be used for the following:
    - Playing games
    - Watching films / programmes / videos
    - Shopping and visiting irrelevant websites

    unless instructed otherwise by a member of staff. If you are caught doing any of the above it will result in a debit. Repeated debits may result in confiscation of the devices for an indefinite period.

2. You should only sign in / log in to your own device and not share your password.

3. Your Chromebook, charger and case are your responsibility. Any damage must be reported straight to Mr Charlton in the IT Office. [Please take care removing or plugging in any USB devices]. If you lose your charger, please contact Mr Charlton and it will be replaced by a genuine charger by the school. Any damage or lost items will be assessed on a case by case basis and any charges for damage deemed avoidable will be charged on end of term bills and parents informed.

4. You may stick **ONE** small and appropriate sticker on the top of the Chromebook to identify it as yours.

5. Headphones should only be used with your Chromebook when permission is given.

6. When transporting your Chromebook it must be in its case and you must not deface or draw on the Chromebook case.

7. You should only get your Chromebooks out when instructed by the teacher. They should remain in your bag until told otherwise. When the Chromebooks are not being used but they are out, the screen **MUST** be closed.

8. Chromebooks **MUST NOT** be used at break or lunch without permission.

9. Documents and Drives should only be created and shared with relevant people and created for school work purposes only.

Name:	Current Year:
Signed:	Date: