Downs View E-Safety Policy

Co-ordinators	**Rachel Mcdonald-Taylor, Jackie Hutchings - DVS Juliet Hudson - Link College Raul Ortiz- Life Skills College**
Date of Completion	**September 2021**
Date of adoption by Governors	**September 2021**
Date of Review	**January 2024**

Contents

1 Policy Rationale

The Designated Child Protection Coordinators will undertake the role of e-Safety Co-ordinators in the organisation. The e-Safety Policy has been developed by the school, building on the Brighton and Hove model e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors; parents have also been made aware of the content. The policy will be reviewed annually.

2 Teaching and learning

2.1 The importance of Internet use

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 Benefits of the Internet to education

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils world-wide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with BHCC and DCSF;
- access to learning wherever and whenever convenient.

2.3 Using the Internet to enhance pupil learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils ie Smoothwall
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught about healthy use of the Internet, frequency and length of time; including making choices during leisure time and having a healthy balance with other non-computer alternatives

2.4 Evaluation of Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3 Managing Information Systems

3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly (including laptops).
- Security strategies will be reviewed regularly with a senior LA technician.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Technical support staff will review system capacity regularly and report their findings to the Business Manager.

3.2 E-mail

3.2.1 Pupil emails

- Pupils may only use approved e-mail accounts, if this has been agreed to be appropriate for them.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations on behalf of the school should be written carefully and with due care and attention.

3.2.2 Staff emails

- Staff emails are requested by the admin team and are administrated by Schools ICT department
- The use of email and attachments follows Brighton & Hove's guidelines.
- Staff **must** use approved email accounts for school purposes.
- Circular emails to parents and other stakeholders should be sent bcc (blind carbon copy) so that email addresses are not disclosed to everyone.
- Emails and their attachments of a sensitive nature should be sent encrypted.
- Push email (*i.e. using an app to manage emails that does not require a* password) to mobile devices will only be permitted after the member of staff has signed a contract and returned it to Schools ICT. (See Appendix D)

3.3 Management of published content

- Information available on the school's VLP will comply with all necessary guidelines.
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses will be published carefully online.
- The Executive Head Teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.4 Publishing of pupil images

Pupils also need to be taught the reasons for caution in publishing personal information and images on social media sites (see section 3.5)

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, unless written parental consent has been given
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents. Please see the safeguarding policy

3.5 Management of social networking

- The school and Smoothwall will filter access to social networking sites. Some may be accessed for specific curriculum activities. Staff will have responsibility for logging off after use. This will be monitored through the staff member's log in.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM, gamer tags and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- School should be aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.

3.5 Web Filtering

- The school will work with BHCC to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator who will then inform Paul Platts at BHCC (see appendix F)
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be reported to DSLs, who will refer to appropriate agencies such as Internet Watchdog Foundation and Paul Platts at BHCC
- The school's filtering strategy will be maintained by the BHCC ICT department.

3.6 Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones should be handed into the class teacher; some pupils in KS4 may keep their mobile phones on them but they must be switched off and not used throughout the school day unless for teaching and learning activities. The sending or sharing of abusive or inappropriate text messages/images/videos is forbidden.
- Some learners in KS5 and Post 19 will be allowed to use their mobile phones during break times. Staff will closely monitor the use of the mobile phones. Learners are not allowed to record, take photos or videos of staff or other learners. If learners cannot follow these rules, then they will not be allowed to use their mobile phones during school/college time, or other recording high tech devices such as watches.

3.7 Protection of personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR.

4 Policy Decisions

4.1 Authorisation to use the Internet

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read the Acceptable Use of ICT policy before using any school ICT resource.
- Selected students must apply for Internet access individually by agreeing to comply with the e-Safety Rules- see contract below
- Parents will be informed that pupils will be provided with supervised Internet access via the school prospectus.

4.2 Risk Assessment

- The school will take all reasonable and possible precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor BHCC can accept liability for the material accessed, or any consequences resulting from Internet use but the school will act immediately to deal with any such incursions.
- The school will, in conjunction with senior LA technicians, audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 E-safety complaints procedure

See also Response to an Incident of Concern (Appendix A)

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Executive Head Teacher and or the LADO depending on the nature of the misuse
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- DSLs will discuss with appropriate bodies which may include the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

5 Communications Policy

5.1 Policy introduction

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be followed as part of the PSHE curriculum to raise awareness and the importance of safe and responsible Internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

5.2 Staff sharing of e-safety policy

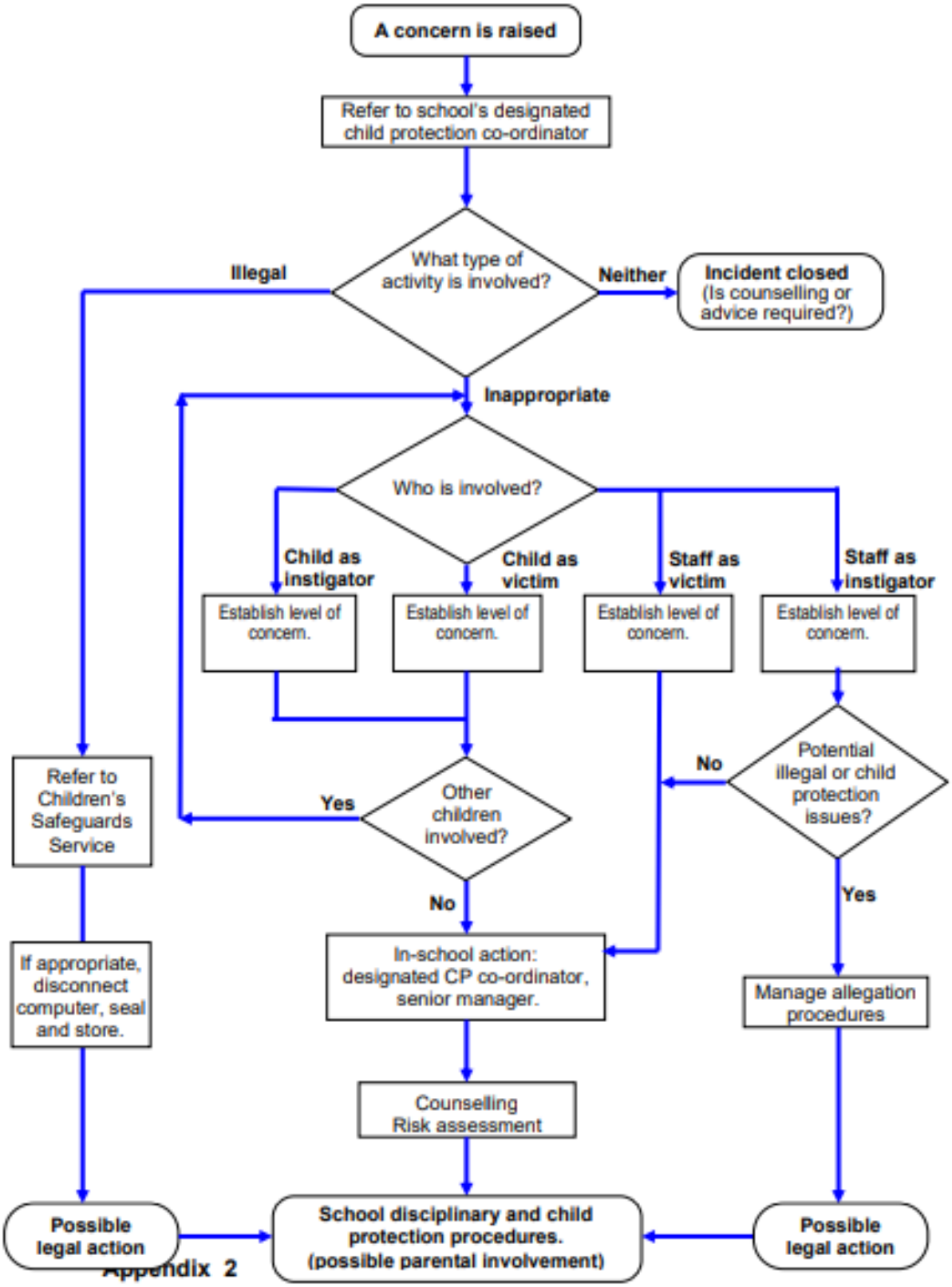
- All staff have access to the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided yearly.

5.3 Parental Involvement

- Parents' attention will be drawn to the school's e-Safety Policy on the school/college website and on the school's VLP.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent coffee mornings with demonstrations and suggestions for safe home internet use.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations deemed suitable by BHCC

Appendix A
Response to an Incident of Concern



Appendix B

Downs View Responsible Internet Use: Rules for Staff and Pupils

This statement is aimed to protect pupils and staff by clarifying what is considered to be acceptable and non-acceptable use of the Internet at Downs View.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the pupils' education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Users are responsible for emails they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Anonymous messages must not be sent.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private purposes unless permission has been given by the Executive Head Teacher.
- Use of the Internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of the school's ICT systems must not be compromised.
- Irresponsible use may result in the loss of internet access.
- The school may exercise its right, by electronic means, to monitor the use of the school's computer systems including the monitoring of web sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it considers unauthorised use of the system may be taking place or where the system may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.
- The risks posed by social networking sites, which involves students, parents and staff, any of whom could unwittingly give away potentially damaging personal information without realising it. Staff should ensure personal details are set to private if using Facebook, or other similar sites which might reveal private information.
- It is known that potential employers and others will search the web for information about job applicants. Unwise postings to social networking sites could come back to haunt older students, staff and parents
- Staff are advised against publishing personal details on social networking sites that may compromise their professional integrity within the school environment.
- Staff must not use the Internet in or out of school for any purpose that may bring the school into disrepute.
- Members of staff should not be interacting with students or parents within a closed, or semi-closed environment e.g. do not use texts, Facebook, Whatsapp or Messenger, personal email, personal mobile to contact

parents. If in doubt, staff should consult their line manager/Child protection team and or the IT Services Dept.

- ♣ All staff to have contact with parents/carers through school Ping, email or telephones. In an emergency, staff can contact parents on their personal mobile (It is advisable to block your number before making the call). However, please use your discretion as the office staff could make the call.
- ♣ Staff who work and support pupils as PAs outside of school/college hours need to tell DSL to keep a record of it

Appendix C

Responsible Internet Use:

For use by selected students

Pupil Agreement

Name of pupil: …….

I agree to abide by the following rules for responsible use of the Internet:

- I will only use my own login and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will only e-mail people I know or whom my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or telephone number or arrange to meet someone.
- I will ask permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat rooms.
- If I see anything I am unhappy about or if I receive messages I do not like, I will tell a member of staff at once.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers in school.

Signed …… Date……

Appendix D

Personal Mobile Phone Agreement:

For use with students where appropriate and needed.

Pupil Agreement

Name of pupil: …….

I agree to abide by the following rules for responsible use of my personal mobile phone:

- I understand that bringing a personal electronic device to school is a privilege that may be taken away if I abuse it.
- Personal electronic devices will be switched off and kept out of sight during lessons, unless the pupil is using the device as part of a lesson with the permission of their class teacher.
- Mobile phones will only be used for voice calls in emergency situations and with the express permission of a member of staff.
- Outside lessons and at break times only, pupils will use soundless features such as text messaging, answering services, call diversion and vibration alert to receive important calls and messages.
- I agree to abide by this agreement and I understand the consequences if I fail to do so.

Signed …… Date……

Appendix E

O365 Mobile Device Email Access Policy and Form

When mobile devices such as Smartphones and Tablets connect to the Schools Email service, via Office 365, they store a local copy of email messages and attachments on your device. In order to minimize risk in the event of theft or loss of mobile devices, it is very important that your device enables reasonable security features including:

1. **Automatically locking your device after a period of inactivity**
2. **Requiring a reasonable passcode to unlock your device** (i.e. not 1111)
3. **Enabling built-in device encryption**
4. **Setting device to self-erase in the event of too many incorrect password attempts**

In accordance with information security policies, the above settings are mandatory on any device that wishes to access school email. This protects your information from abuse by unknown and unauthorised persons.

All staff accessing school email data (email, calendar, and contacts) on a mobile device will be required to accept the schools mobile device access policy.

You will be prompted to create a password on your mobile device. After you unlock your phone, you will be prompted to enter your password. Please note that your device will also lock after a period of inactivity.

What happens if my device is lost or stolen?

If your phone is lost or stolen, you must inform ICT Schools & Traded Services Team and your school as soon as possible. Upon you informing us, the following will happen:

- **Your account will be disabled for mobile use.**
- **Your mobile device will be wiped remotely.** This will perform a factory reset on your phone and delete all data, i.e. emails, photos, music etc.

What should I do if I give away or sell my phone?

- You must perform a factory reset on your phone.

Staff Agreement		
I certify I have read the statements above and agree to the mobile device policy. I understand I must report my phone lost or stolen to ICT Schools & Traded Services and my school as soon as possible and that my phone will be data wiped.		
School name:		
Staff member name: *(CAPS)*		
Staff member email address:		
Staff member signature:		

As your Headteacher is the Data Controller for your school, they will need to provide authorisation for you to receive emails on your mobile device.

Headteacher Agreement		
Headteacher name: *(CAPS)*		
Headteacher signature:		Date:

Return this form either by post or email using the details below. Guidance will be sent to you by return.

Email: ictsts@brighton-hove.gov.uk | **Post:** ICT Schools & Traded Services**,** Brighton & Hove City Council, 4th Floor, Bartholomew House, Bartholomew Square, Brighton BN1 1JE

ICT Schools & Traded Services

Service desk: 01273 293663 I ictsts@brighton-hove.gov.uk I twitter @BHCC_ICT

June.20 2018

Appendix F

e-Safety Contacts and References

- **Site DSLs:** DVS – Jackie Hutchings and Rachel Mcdonald-Taylor
  DVLC – Juliet Hudson
  DVLSC – Raul Ortiz

- **DfE guidance - Teaching online safety in school:** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

- **CEOP (Child Exploitation and Online Protection Centre):** www.ceop.police.uk

- **e–Safety Officer for Brighton & Hove:** Paul Platts - paulplatts@brighton-hove.gov.uk

- **Childline:** www.childline.org.uk

- **Childnet:** www.childnet.com

- **Click Clever Click Safe Campaign:** http://clickcleverclicksafe.direct.gov.uk

- **Cybermentors:** www.cybermentors.org.uk

- **Digizen:** www.digizen.org.uk

- **Internet Watch Foundation (IWF):** www.iwf.org.uk

- **Kidsmart:** www.kidsmart.org.uk

- **Think U Know:** www.thinkuknow.co.uk

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