Chafyn Grove School

eSafety Policy

1. INTRODUCTION

This policy supports the aims of the School in educating Chafyn Grove pupils to explore their horizons in line with the e-world safely, and in setting up a safety net around them.

This policy focusses on the area of eSafety within the school, and any remote working, but should be considered alongside the Computer Usage Policy as good practice in ICT use underpins the eSafety efforts within the school.

2. RATIONALE

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Chafyn Grove, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Computer Usage Policy are inclusive of both fixed and mobile internet; technologies provided by the school such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc; and technologies owned by

pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

3. MONITORING

The school maintains the right, through authorised ICT staff to monitor any equipment used on the school site. This provision is made to ensure that we have the capability to ensure that members of the school community are not being exposed to, or subjected to, any behaviour that risks their eSafety.

Where there is a concern regarding the nature of network traffic or content, the incident will be logged by the ICT team and referred via Child Protection routes to the Designated Safeguarding Lead or Headmaster as dictated by the Child Protection Policy. If the logged event concerns a member of staff, this will be confidentially referred to the Headmaster. In the event that the Headmaster should be the subject of a concern, reports should be made to the Chair of Governors.

All eSafety concerns, if forwarded, are logged and any occasion when access is made to a user's account are also logged with time, date and reason by the Network Manager. There is provision through the local hardware appliance for filtering, whereby safeguarding concerns are forwarded as alerts directly to the DSL and Headmaster.

The school, through the internet filter, operates a safeguarding program which monitors records and alerts staff to breaches of policy.

4. BREACHES OF POLICY

4.1 Incident Reporting

All eSafety incidents involving either staff or pupils generate an alert to the Headmaster (for staff) or DSL (for students) and are logged within the Safeguard system that is in place alongside the internet filter.

4.2 Complaints

Complaints and/or issues relating to eSafety should be made to the Pastoral Deputy head or DSL. Incidents should be logged and the School procedure for investigating an eSafety incident should be followed.

4.3 Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the DSL.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the DSL, depending on the seriousness of the offence; investigation by the Director of Pastoral Care/Headmaster, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

Where a pupil is found to have accessed or searched for inappropriate material, their user account will be locked for a period of time, whilst they are spoken to by the DSL, Director of Pastoral Care or Head of ICT about their use of the computers.

5. INCLUSION

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

6. ROLES AND RESPONSIBILITIES

As eSafety is an important aspect of strategic leadership within the school, the Headmaster and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. **The named DSL in this school is Lynsey Hearsey, who is also the Pastoral Deputy Head**. All members of the school community have been made aware of who holds this post.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the school policies listed in the introduction to this policy.

The ICT Staff who are involved in securing the network and monitoring are Paula Mortimer (Network Manager) and Michael Spice (Head of ICT).

The Headmaster, Simon Head also receives alerts for inappropriate use of the computers.

7. STUDENT AND STAFF EDUCATION AND TRAINING

7.1 eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. ESafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

Pupils are informed of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as ChildLine or CEOP report abuse button.

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

7.2 eSafety Skills Development for Staff

New staff receive information on the school's acceptable use policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Our staff receive regular information and training on eSafety issues in the form of INSET from the DSL or a nominated person.

8. SYSTEMS AND ACCESS

8.1 eSafety on the Internet

On our network we maintain a number of filters to secure our network and keep its users as safe as possible.

For network traffic, we use recommendations to employ industry leading filters and hardware appliances which monitor email as well as internet traffic content.

The local, hardware appliance includes a link to reporting software which raises alerts to the members of staff listed in section 6.

These systems are kept up to date and monitored by the Network Manager. **Names of providers are removed from this document as it is publicly visible. Information in the event of audit/inspection is available from the Network Manager or Head of ICT.

8.2 Online Communication

The school recognises the benefit of online communication for the development of knowledge, sharing of information and communication between school and home. As such, we make the following allowances for online communication.

Pupils have access to Office365 services online, through their own personal account. These are primarily available for home schooling, but may be used in lessons to facilitate digital work. The children are made aware that these accounts are subject to monitoring and that they can be audited in the case of a concern. The children do not have access to an email account so as to keep communication internal.

Staff are given training and advice on how to use the emails when they are inducted as new staff.

The boarding house maintains a Skype account which is connected to the shared iPads, this enables the children to contact their parents in the evening. By using a shared account, we are able to monitor who is contacted from the account to ensure the safety of the children using it.

The children are not given access to any social media platforms, staff may have some access, but the acceptable use of these platforms is covered within the Code of Practice that all staff sign up to.

8.3 Remote Working

The school has the facility to teach remotely through the Microsoft Teams platform, which all children have access to. Staff access is maintained on a multi-factor authentication basis to ensure security of the data within. Pupils have all been given advice on how to set secure and useful passwords. They have no access to email through the platform.

During the course of remote learning, there may be the necessity to hold a video meeting. The following guidance has been given to staff and pupils regarding how they should interact when using video online. The approved platforms are Teams (preferable) and Zoom (if parents are helping).

Video Conferencing Guidelines.

Teacher Expectations.

- Teacher will only use school approved video conferencing platforms (Microsoft Teams and Zoom)
- Teachers will only use these applications (Zoom & Team) with their school provided email
- Teachers will contact parents and students through the Chafyn Grove School email only
- Teachers will make their HOD or SMT aware of regular scheduled online meetings.
- If conducting an instructional video session in Teams, teachers should use the 'record' option, so that absent students can view the video content on Google classroom, at a later date.
- Teachers will keep a record of each Meeting online (including date, time, length, attendees and topics covered)
- Online Meetings will be kept to a reasonable time period, as devices and Internet may be in high demand at home. (e.g. class length)
- Teachers will aim to ensure students join the meeting with camera and microphones muted on entry.
- Teachers will ensure the students abide by Schools Internet Acceptable Usage Policy at all times.
- Teachers must conduct sessions in a professional manner, including being suitably attired during online sessions.
- Where possible video cameras should be used against a neutral background, with the light source directed towards the instructors face.
- It is recommended that teachers wear headsets, ideally with a boom microphone if possible, to limit audio interruptions during conferencing sessions.
- At the end of a session the teacher must advise all students to leave the session and when all students have left the Meet, the teacher can then end the video conferencing and terminate the meeting.

Student/Parent Expectations.

- Only students who have received parental approval may participate in online video conferences.
- Be ontime for your video conference.
- Use the bathroom and eat before (not during) your session.
- Students should be ready with their class resources, pen and paper (or a musical instrument, etc) and be suitably dressed prior to the beginning of each scheduled video conference.
- Where possible, any computers or devices should be used in appropriate areas, for example, a living room, not in a bedroom)
- Keep your video conferencing device on a secure surface, such as a table
- Make sure your device is charged and plugged in.
- If possible, students should wear a headset if available (ideally with a microphone)
- Students will continue to abide by the schools Acceptable Usage Policy during sessions
- Chat functions should be used to ask questions and to answer teacher questions.
- Students will use chat functions responsibly and when directed by the teacher.

- Raise your hand if you have a question and use hand gestures to show understanding such as, thumbs up, or touching your ear, for audio issues.
- Students should listen, focus and learn (Avoid distractions, eg such as mobile phone usage etc)
- Students who continue to fail to abide by the conferencing guidelines, may be muted, or removed from the online meeting.
- Do you best, as in class. Good luck with your online learning.

8.4 Video & Images

The school has the right to take photographs of the children for use in marketing materials and within work, but there are restrictions upon how these photos are taken to ensure that the children are kept safe.

The school provides cameras that are owned and maintained by the school as no staff should use personal photography equipment to take photographs of pupils. This is referred to in the Acceptable Use Policy that all staff sign up to.

On the rare and exceptional occasion where a photograph has to be taken on a staff device, in cases of emergency need, the photograph must be removed immediately after it has been shared with the relevant people. The staff member must ensure the photo is not still in existence on cloud services such as iCloud. The school encourages the use of apps that do not access the camera roll.

No cameras should ever be used in changing rooms or in the boarding house bedrooms when children are, or could be present. When taking photographs of swimming events, heed should be paid to the safety of the children.

8.5 Data Storage and Processing

The school takes its compliance with the Data Protection Act 1998 seriously.

Staff and pupils are expected to save all data relating to their work to their school laptop/ PC or to the school OneDrive/Office365 servers.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending. The school does, however, strongly discourage the use of removable media.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head of ICT or Network Manager who will escalate as required.

9. GUIDING LEGISLATION

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

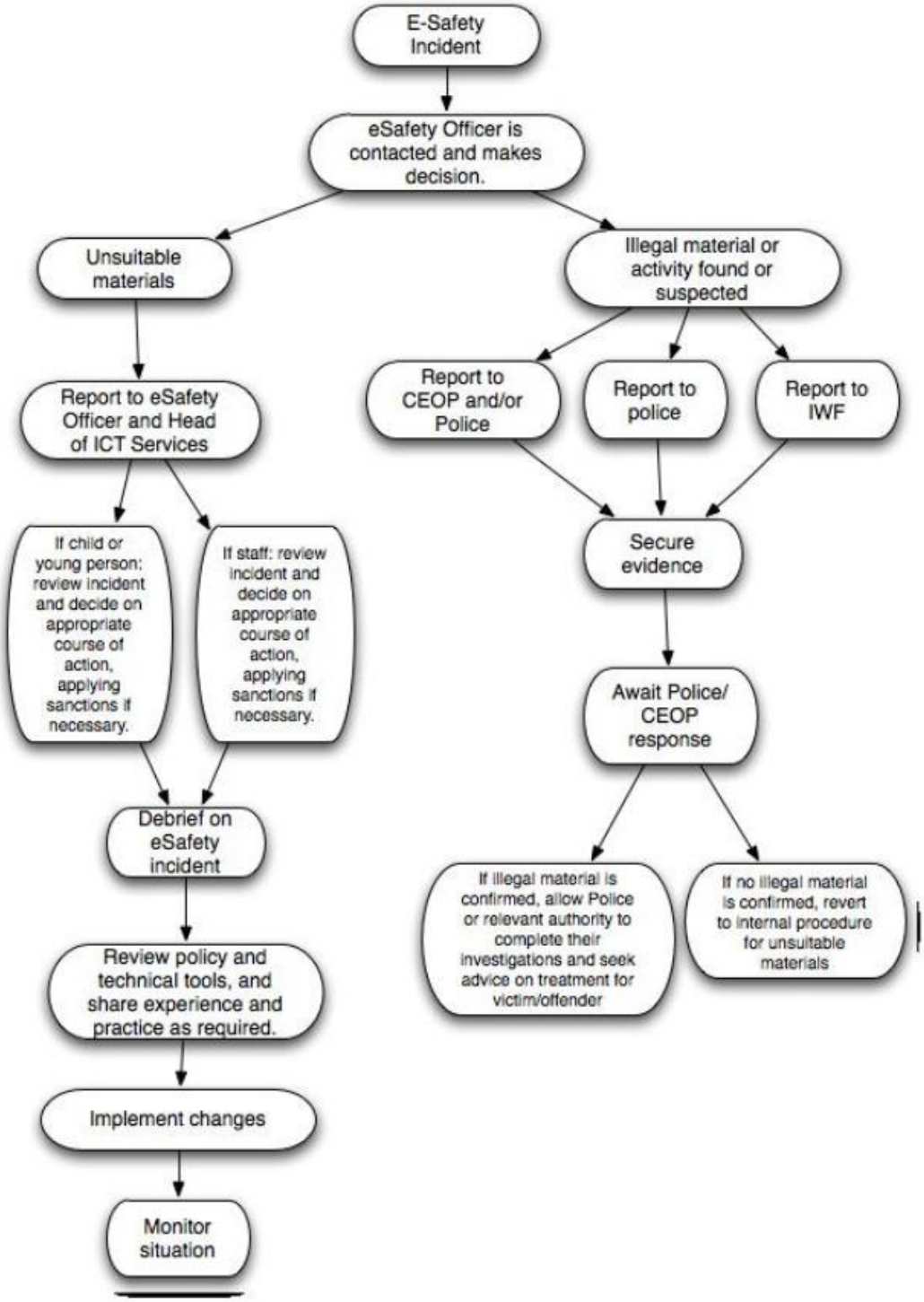
Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Keeping Children Safe in Education 2016 (Annex C)
Briefing from the DfE on Online Safety for Children. Contains guidance on the measures that should be put in place to ensure the safety of children when online.

APPENDIX 1: FLOWCHART FOR RESPONDING TO E-SAFETY INCIDENTS (Adapted from BECTA model in AUPs in Context – Feb 2009)



APPENDIX 4: EXAMPLE OF E-SAFETY INCIDENT LOG

Details of ALL eSafety incidents to be recorded by the eSafety Officer. This incident log will be monitored termly by the Head, Deputy Head (Welfare) Assistant Head (ICT) or Chair of Governors. Any incidents involving Cyber bullying should be recorded in the Bullying Log.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons