Title:	E-Safety Policy
Date of Last Review:	March 2019
Date of Ratification by Governing Body:	May 2019
Status:	Guidance
Approval Authority:	Student Committee
Staff Lead:	Ben Ford
Governor Lead:	Chair of Student Committee
Review Frequency:	Every two years
Location:	Website
Date of Next Review:	March 2021

Rationale

In 2019 most young people have grown up with internet-enabled technology in their home and school. Many will have had early access to smartphones and similar devices that can be used outside the home and in their bedrooms. The use of the internet and social media can have many advantages, but can also pose many threats and dangers when used incorrectly. Over recent years, there have been a number of studies and reports highlighting the growing importance of E-Safety amongst young people. A 2017 Ofcom report stated that almost 1 in 4, 8 to 11 year olds and 3 in 4, 12 to 15 year olds have a social media profile. In 2017/2018, there were 2200 counselling sessions with young people about online sexual abuse and in a 2018 Ofcom report, around 1 in 8 young people were reported to have been bullied online or through social media. These statistics highlight the need for appropriate e-safety policies and procedures to be put in place within schools in order to support and protect our students.

Introduction

In 2007 the government commissioned from Dr Tanya Byron, a review of the risks that children face when using the internet and video games. Subsequently the 'Byron Review' was published, setting out a challenging agenda for the Government, its partners, industry and the third sector, to work together to make children safer when using the internet and video games. The Government accepted all of Dr Byron's recommendations in full, signifying a commitment to children's safety when using new technology. Due to technological advances, E-Safety has become more and more important as new technology, devices and ever younger students immerse themselves in the online world.

Following this, in February 2019, the Government published a report on 'Screen-based activities and young people's mental health and psychosocial wellbeing' which included a guide to parents on supporting young people's use of the internet and social media.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In this case, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place in or out of school.
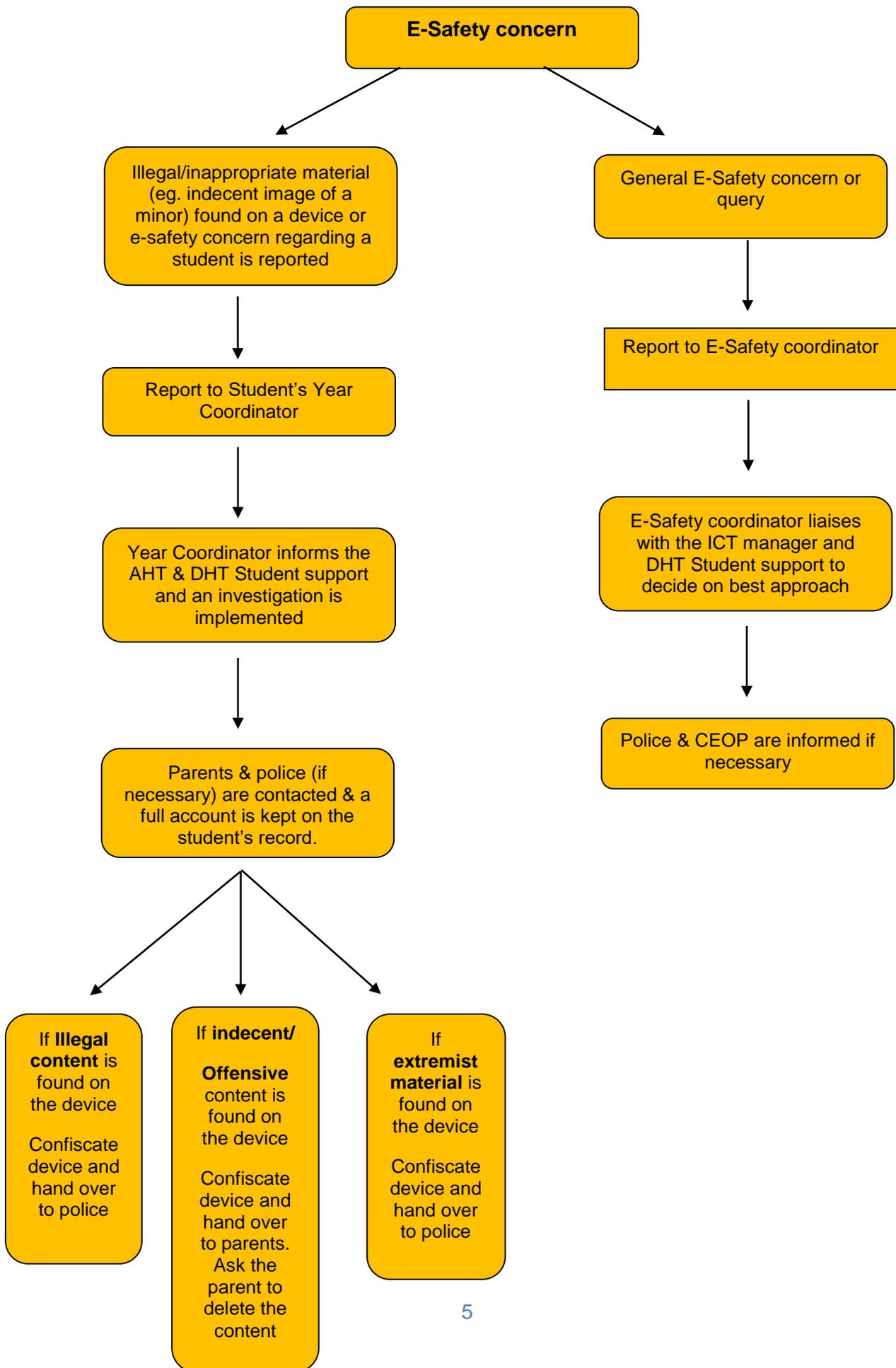
This E-Safety policy applies to all adults, including volunteers, working in or on behalf of our school, and is a document which demonstrates how everyone working in or for our school shares a commitment to keeping children safe from harm and abuse whilst being online or using new technologies

Responsibilities

Staff member	Responsibilities
Governors	• Governors are responsible for the ratification of the E-Safety Policy and for reviewing the effectiveness of the policy.
Headteacher	• The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-Safety Co-ordinator • The Headteacher and Deputy Headteacher, Student Support should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. • 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 online safety roles and to train other colleagues, as relevant. • The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
E-Safety Coordinator	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • Provides training and advice for staff & parents • Liaises with school technical staff • Provides assemblies to all year groups on current e-safety issues. • Receives reports of online safety incidents and alongside the Deputy Headteacher, Student Support, creates a log of incidents to inform future online safety developments • Meets regularly with Deputy Headteacher, Student Support to discuss current issues, review incident logs and filtering / change control logs • Reports regularly to the Senior Leadership Team • Meets with the Deputy Headteacher, Teaching and Learning to ensure that E-Safety is delivered and embedded across the curriculum throughout the academic year.
ICT Technical Manager & technical staff	• Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack • That the school meets required online safety technical requirements and any Local Authority Online Guidance that may apply. • Network users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. • The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person • That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That monitoring software / systems are implemented and updated as agreed in school policies
Teaching staff/ Support staff	• Staff must report any online malicious or offensive material about themselves to the Deputy Headteacher, Student Support and not approach the student directly. Screenshots should be kept and passed to the Deputy Headteacher, Student Support as evidence.

	- Staff must attend Safeguarding training every year to familiarise themselves with the school policies on the safe use of ICT - They have read, understood and signed the Staff Acceptable Use Policy. - They report any suspected misuse or problem to one of the school's safeguarding Designated Teachers. - All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems in line with the school's acceptable use of ICT policy and staff code of conduct. - Online safety issues are embedded in all aspects of the curriculum and other activities - Monitor the use of digital technologies, mobile devices, cameras and other digital devices in lessons and other school activities (where allowed) and implement current policies with regard to these devices. - In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
Designated Safeguarding Lead	- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from: - sharing of personal data - access to illegal / inappropriate materials - inappropriate on-line contact with adults / strangers - potential or actual incidents of grooming - cyber-bullying - Responsible for reporting any incidents to the appropriate authorities & following up on incidents to a satisfactory level.
Students	- Are responsible for using the school digital technology systems in accordance with the ladder of consequence and in line with the school policies. - Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so - Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying. - Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's ladder of consequence* covers their actions out of school, if related to their membership of the school.
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' evenings, newsletters, letters, parent info on the school website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: - digital and video images taken at school events. - access to Parents' section of the website and Show My Homework - Reading appropriate information sent home on E-Safety issues. - Should there be an issue, parents should not approach the children directly but go through the appropriate Year Coordinator or Form Tutor.

Appendix 1: Procedure for reporting concerns

```
                          ┌─────────────────────────┐
                          │     E-Safety concern    │
                          └─────────────────────────┘
                           /                        \
                          /                          \
        ┌──────────────────────────┐      ┌──────────────────────────┐
        │ Illegal/inappropriate    │      │ General E-Safety concern │
        │ material (eg. indecent   │      │ or query                 │
        │ image of a minor) found  │      └──────────────────────────┘
        │ on a device or           │                  │
        │ e-safety concern         │                  ▼
        │ regarding a student is   │      ┌──────────────────────────┐
        │ reported                 │      │ Report to E-Safety       │
        └──────────────────────────┘      │ coordinator              │
                     │                     └──────────────────────────┘
                     ▼                                 │
        ┌──────────────────────────┐                  ▼
        │ Report to Student's Year │      ┌──────────────────────────┐
        │ Coordinator              │      │ E-Safety coordinator     │
        └──────────────────────────┘      │ liaises with the ICT     │
                     │                     │ manager and DHT Student  │
                     ▼                     │ support to decide on     │
        ┌──────────────────────────┐      │ best approach            │
        │ Year Coordinator informs │      └──────────────────────────┘
        │ the AHT & DHT Student    │                  │
        │ support and an           │                  ▼
        │ investigation is         │      ┌──────────────────────────┐
        │ implemented              │      │ Police & CEOP are        │
        └──────────────────────────┘      │ informed if necessary    │
                     │                     └──────────────────────────┘
                     ▼
        ┌──────────────────────────┐
        │ Parents & police (if     │
        │ necessary) are contacted │
        │ & a full account is kept │
        │ on the student's record. │
        └──────────────────────────┘
           /          │          \
          /           │           \
```

If Illegal content is found on the device

Confiscate device and hand over to police

If **indecent/**

Offensive content is found on the device

Confiscate device and hand over to parents. Ask the parent to delete the content

If **extremist material** is found on the device

Confiscate device and hand over to police

Appendix 2: Sanctions for inappropriate use of ICT

School sanctions for inappropriate usage of ICT will be in line with the school's ladder of consequence.

During lessons (including form time and cover lessons)		Outside lessons
5 Behaviour	• Behaviour likely to incite disorderly conduct in school including inappropriate expression of extremist views.	• Bringing the school into disrepute, • Dishonesty, • Behaviour likely to incite disorderly conduct in school. • Malicious use of social media and misuse of ICT
C5	**Refer to HOF inform by email to YCO/Senior Detention/Internal Exclusion**	**REFERRAL TO YCO/AHT. Monitoring group/PSP/Referral to external agencies. Senior Detention/Internal Exclusion/Curfew Detention**
C6 Behaviour	• bullying/intimidation/inappropriate sexual behaviour (may be C7 at the discretion of AHT), • Prejudice based bullying.	
C6	**INTERNAL EXCLUSION/FIXED TERM EXCLUSION – DHT/AHT**	