Online Safety Procedure

COOMBE HOUSE
SCHOOL

Procedure owner:	Designated Safeguarding Lead	**Adoption Date:**	January 2023
Approved by company:	Managing Director		
Review cycle:	Annual		
Last reviewed on:	December 2023		
Changes made:	Annual Review		
Next review due by:	December 2024		

Dorset
Centre of
Excellence

Contents

1	Aims	3
2	Scope and application	3
3	Regulatory framework	3
4	Publication and availability	4
5	Definitions	4
6	Responsibility statement and allocation of tasks	5
7	Role of staff and parents	5
8	Access to the School's technology	8
9	Procedures for dealing with incidents of misuse	9
10	Education	11
11	Training	12
12	Cybercrime	14
13	Risk assessment	15
14	Record keeping	15
15	Version control	15

1 Aims

1.1 This is the online safety procedure of Coombe House School (the "School").

1.2 The aim of this procedure is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

1.2.1 protects the whole School community from illegal, inappropriate and harmful content or contact;

1.2.2 educates the whole School community about their access to and use of technology;

1.2.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate; and

1.2.4 to help to promote a whole school culture of openness, safety, equality and protection.

1.3 This procedure forms part of the School's whole school approach to promoting child protection, safeguarding and wellbeing, which seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

1.4 Online safety is a running and interrelated theme throughout many of the School's policies and procedures (including its safeguarding and child protection policy and procedures) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, staff training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Leads.

2 Scope and application

2.1 This procedure applies to the whole School.

2.2 This procedure applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

3 Regulatory framework

3.1 This procedure has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 Education and Skills Act 2008;

3.1.3 Children Act 1989

3.1.4 Childcare Act 2006

3.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (**UK GDPR**); and

3.1.6 Equality Act 2010.

3.2 This procedure has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2023) (**KCSIE**);

3.2.2 Preventing and tackling bullying (DfE, July 2017);

3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, December 2020);

3.2.4 Revised Prevent duty guidance: for England and Wales (Home Office, December 2023);

3.2.5 Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism (Home Office, February 2021);

3.2.6 Searching, Screening and Confiscation: Advice for schools (DfE, July 2022);

3.2.7 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, September 2021);

3.2.8 Teaching online safety in schools (DfE, January 2023);

3.2.9 Harmful online challenges and online hoaxes (DfE, February 2021);

3.2.10 Online safety guidance if you own or manage an online platform (DfDCMS, June 2021);

3.2.11 A business guide for protecting children on your online platform (DfDCMS, June 2021); and

3.2.12 Online safety audit tool (UKCIS, October 2022).

3.3 The following School policies, procedures and resource materials are relevant to this procedure:

3.3.1 Staff IT acceptable use policy and social media policy

3.3.2 Safeguarding and child protection policy and procedures

3.3.3 Anti-bullying policy

3.3.4 Risk assessment

3.3.5 Staff code of conduct and whistleblowing policy

3.3.6 Data protection policy for staff

3.3.7 Sex and relationships education policy

4 Publication and availability

4.1 This procedure is made available to all staff and other stakeholders. This procedure is available in hard copy on request.

4.2 A copy of the procedure is available for inspection from the school office during the School day.

4.3 This procedure can be made available in large print or other accessible format if required.

5 Definitions

5.1 Where the following words or phrases are used in this procedure:

5.2 References to the **Proprietor** are references to Dorset Centre of Excellence Limited.

5.3 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this procedure as **technology**).

6 Responsibility statement and allocation of tasks

6.1 The Proprietor has overall responsibility for all matters which are the subject of this procedure.

6.2 The Proprietor is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this procedure is part of the Proprietor's response to this duty.

6.3 To ensure the efficient discharge of its responsibilities under this procedure, the Proprietor has allocated the following tasks:

Task	**Allocated to**	**When / frequency of review**
Keeping the procedure up to date and compliant with the law and best practice	Designated Safeguarding Lead	As required, and at least annually
Monitoring the implementation of the procedure (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	Headteacher	As required, and at least annually
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the procedure	Headteacher	As required, and at least annually
Formal annual review	Managing Director	Annually

7 Role of staff and parents

7.1 Head and Senior Leadership Team

7.1.1 The Head has overall executive responsibility for the safety and welfare of members of the School community.

7.1.2 The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of technology in the

same way as other safeguarding matters, in accordance with the School's safeguarding and child protection policy and procedures.

7.1.3 The Designated Safeguarding Lead will work with the School's IT provider, Dorset Council, in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

7.1.4 The Designated Safeguarding Lead will regularly monitor the prevalence of online safety related issues, in liaison with the IT technician.

7.1.5 The Designated Safeguarding Lead will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

7.2 **IT technician**

7.2.1 The IT technician, together with their team, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

7.2.2 The IT technician is responsible for ensuring that:

(a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the School's technology if they are properly authenticated and authorised;

(c) the School has an effective filtering procedure in place and that it is applied and updated on a regular basis;

(d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

(e) the use of the School's technology is regularly monitored to ensure compliance with this procedure and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the IT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

7.2.3 Dorset Council provide internet connectivity and filtering.

7.2.4 The IT technician will report regularly to the Senior Leadership Team on the operation of the School's technology. If the IT technician has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the Designated Safeguarding Lead or another relevant member of the leadership team.

7.2.5 The IT technician is responsible for maintaining suitable records and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's safeguarding and child protection policy and procedures.

7.3 **All staff**

7.3.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies/procedures and of safe practice with the pupils.

7.3.2 Staff are expected to adhere, so far as applicable, to each of the policies and procedures referenced in this procedure.

7.3.3 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

7.3.4 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content;

(d) cyberbullying.

7.3.5 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and/or encourages physical abuse;

(b) facilitates, threatens and/or encourages sexual violence; or

(c) is used as part of initiation/hazing type violence and rituals.

7.3.6 It is important that staff recognise the indicators and signs of child on child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child on child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported; a stance of 'it is happening here' is taken.

7.3.7 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain online behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse.

7.3.8 The School has a **zero tolerance approach** towards online child on child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's behaviour policy and procedures and also as a safeguarding matter under the School's safeguarding and child protection policy and procedures.

7.3.9 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this procedure and the School's safeguarding and child protection policy and procedures. If staff have any concerns regarding child on child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the Designated Safeguarding Lead in all cases**.

7.4 **Parents and carers**

7.4.1 The role of parents and carers in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents and carers to promote safe practice when using technology and to:

(a) support the School in the implementation of this procedure and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

7.5 **If parents or carers have any concerns or require any information about online safety, they should contact the School who will offer support and advice.**

8 Access to the School's technology

8.1 The School provides IT systems to pupils and staff as well as other technology. All such use is monitored by the IT team.

8.2 Pupils and staff require individual usernames and passwords to access the School's IT systems which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their usernames or passwords must report it to the IT team immediately.

8.3 No laptop or other mobile electronic device may be connected to the School network without the consent of the company. The use of any device connected to the School's network will be logged and monitored by the IT team. See also 8.5 below.

8.4 The School has a separate wireless network connection available for use by visitors to the School.

8.5 **Inappropriate material**

8.5.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

8.5.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead. The term 'online safety' encapsulates a wide range of issues but these can be classified into four main areas of risk:

(a) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism);

(b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, commercial advertising and adults posing as

children or young adults with the intention to groom and / or exploit them for sexual, criminal, financial or other purposes);

(c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and online bullying; and

(d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

8.6 **Use of mobile electronic devices and smart technology**

8.6.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet when connected to the School's network. Mobile devices and smart technology equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. The School is alert to the risks that such access presents, including the risk of pupils sexually harassing their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually; or viewing and/or sharing pornography and other harmful content, and has mechanisms in place to manage such risks.

8.6.2 In certain circumstances, a pupil may be given permission to use their own mobile device or other smart technology to connect to the internet using the School's network. Permission to do so must be sought and given in advance.

8.6.3 The use of mobile electronic devices by staff is covered in the code of conduct, IT acceptable use policy and data protection policy for staff (including remote working and bring your own device to work).

8.6.4 The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

9 Procedures for dealing with incidents of misuse

9.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this procedure and the School's safeguarding and disciplinary policies and procedures.

9.2 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to shared further (e.g. with the Designated Safeguarding Lead) to discuss next steps.

9.3 **Misuse by pupils**

9.3.1 Anyone who has any concern about the misuse of technology by pupils should report it immediately so that it can be dealt with in accordance with the School's behaviour policies and procedures, including the anti-bullying policy where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-bullying	Headteacher or any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Sharing nudes and semi-nude images (sexting/ youth produced sexual imagery)	Safeguarding and child protection policy	Headteacher Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Sexual violence and sexual harassment (whether during or outside of school)	Safeguarding and child protection policy	The Designated Safeguarding Lead who has overall responsibility for online safety matters
Harassment	Safeguarding and child protection policy	Headteacher Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Upskirting	Safeguarding and child protection policy	Headteacher Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Radicalisation	Safeguarding and child protection policy	Headteacher Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters

9.3.2 **Anyone** who has **any** concern about the welfare and safety of a pupil must report it **immediately** in accordance with the School's child protection procedures.

9.4 **Misuse by staff**

9.4.1 Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the appropriate procedures.

9.4.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's safeguarding and child protection policy and procedures.

9.5 **Misuse by any user**

9.5.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the IT technician or the Designated Safeguarding Lead.

9.5.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9.5.3 If the School considers that any person is vulnerable to radicalisation and meets the criteria, the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may also report it directly to the police.

10 Education

10.1 The safe use of technology is integral to the School's curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices (see the School's curriculum policy).

10.2 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities, teaching pupils:

10.2.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

10.2.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";

10.2.3 to be critically aware of content they access online and guided to validate accuracy of information;

10.2.4 how to recognise suspicious, bullying or extremist behaviour;

10.2.5 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

10.2.6 the consequences of negative online behaviour;

10.2.7 how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

10.2.8 how to respond to harmful online challenges and hoaxes.

10.3 Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The School has a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences under the School's behaviour policy and procedures and if necessary as a safeguarding matter under the School's safeguarding and child protection policy and procedures.

10.4 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

10.5 **Useful online safety resources for pupils**

10.5.1 http://www.thinkuknow.co.uk/

10.5.2 http://www.childnet.com/young-people

10.5.3 https://www.saferinternet.org.uk/advice-centre/young-people

10.5.4 http://www.safetynetkids.org.uk/

10.5.5 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

10.5.6 https://www.bbc.com/ownit

10.5.7 https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people

11 Training

11.1 Staff

11.1.1 The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

11.1.2 Induction training for new staff includes training on the School's online safety training modules, the staff code of conduct, staff IT acceptable use policy and social media policy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes.

11.1.3 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology., and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

11.1.4 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images. Staff are aware of the procedures for Searching, Screening and Confiscation: Advice for schools (DfE, July 2022). In certain cases, it may be appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection in line with the guidance above.

11.1.5 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' or ‘it is happening here’ in relation to sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and / or violent behaviour in the future.

11.1.6 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to

whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and/or staff training will be delivered to minimise the risk of it happening again.

11.1.7 Staff also receive data protection and cyber-security training on induction and at regular intervals afterwards.

11.1.8 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

11.1.9 **Useful online safety resources for staff**

(a) http://swgfl.org.uk/products-services

(b) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

(c) http://www.childnet.com/teachers-and-professionals

(d) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(e) https://www.thinkuknow.co.uk/teachers/

(f) http://educateagainsthate.com/

(g) https://www.commonsense.org/education/

(h) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)

(i) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

(j) Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, December 2020).

(k) Online safety in schools and colleges: questions from the governing board (UKCIS, October 2022)

(l) Education for a connected world framework (UKCIS, 2020)

(m) https://www.lgfl.net/online-safety/resource-centre

(n) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

(o) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

(p) SELMA Hack online hate toolkit (SWGFL, May 2019)

(q) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, January 2023)

(r) Harmful online challenges and online hoaxes (DfE, February 2021)

(s) Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.

(t) NSPCC helpline for anyone worried about a child - 0808 800 5000

(u) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

11.1.10 The local safeguarding partnership has produced guidance for parents on radicalisation.

11.2 **Parents and carers**

11.2.1 **Useful online safety resources for parents and carers**

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

(b) http://www.childnet.com/parents-and-carers

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(d) https://www.thinkuknow.co.uk/parents/

(e) http://parentzone.org.uk/

(f) https://www.internetmatters.org/

(g) https://www.commonsensemedia.org/

(h) Advice for parents and carers on cyberbullying (DfE, November 2014)

(i) http://www.askaboutgames.com

(j) https://www.ceop.police.uk/safety-centre

(k) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

(l) LGfL: parents - scare or prepare

(m) Thinkuknow: what to do if there's a viral scare online

12 Cybercrime

12.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

12.2 12.2 Cyber-dependent crimes include:

12.2.1 unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

12.2.2 denial of service (Dos or DDoS) attacks or 'booting', which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

12.2.3 making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

12.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

12.4 If staff have any concerns about a child in this area, they should refer the matter to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

13 Risk assessment

13.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

13.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans . Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

13.3 The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

13.4 Day to day responsibility to carry out risk assessments under this procedure will be delegated to senior staff who have/has been properly trained in, and tasked with, carrying out the particular assessment.

14 Record keeping

14.1 All records created in accordance with this procedure are managed in accordance with the School's policies that apply to the retention and destruction of records.

14.2 All serious incidents involving the use of technology will be logged centrally by the School.

14.3 The records created in accordance with this procedure may contain personal data. The School has a number of privacy notices which explain how the School will use personal data. The School's approach to data protection compliance is set out in the Data Protection Policy. In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this procedure; this includes the School's Data Protection Policy.

15 Version control

Date of adoption of this procedure, by or on behalf of the Proprietor	January 2023
Date of last review of this procedure	December 2023
Date for next review of this procedure	December 2024
Procedure owner (Proprietor)	Dorset Centre of Excellence