Online safety policy

Coventry Extended Learning Centre



|  |  |  |
| --- | --- | --- |
| **Approved by:** | Glenn Mellor | **Date:** 18 September 2022 |
| **Last reviewed on:** | 18/09/2022 | |
| **Next review due by:** | 04/09/2023 | |

**Contents**

[1. Aims 3](#_Toc20749256)

[2. Legislation and guidance 3](#_Toc20749257)

[3. Roles and responsibilities 3](#_Toc20749258)

[4. Educating pupils about online safety 5](#_Toc20749259)

[5. Educating parents about online safety 6](#_Toc20749260)

[6. Cyber-bullying 6](#_Toc20749261)

[7. Acceptable use of the internet in school 8](#_Toc20749262)

[8. Pupils using mobile devices in school 8](#_Toc20749263)

[9. Staff using work devices outside school 8](#_Toc20749264)

[10. How the school will respond to issues of misuse 9](#_Toc20749265)

[11. Training 9](#_Toc20749266)

[12. Monitoring arrangements 9](#_Toc20749267)

[13. Links with other policies 10](#_Toc20749268)

[Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers) 11](#_Toc20749270)

[Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 12](#_Toc20749271)

[Appendix 3: online safety training needs – self audit for staff 13](#_Toc20749272)

[Appendix 4: online safety incident report log 14](#_Toc20749273)

# 1. Aims

Our school aims to:

* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
* Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
* Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

* **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
* **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

# 2. Legislation and guidance

This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on:

* [Teaching online safety in schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)
* [Preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [cyber-bullying: advice for headteachers and school staff](https://www.gov.uk/government/publications/preventing-and-tackling-bullying)
* [Relationships and sex education](https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education)
* [Searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation)

It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

# 3. Roles and responsibilities

3.1 The management committee

The management committee has overall responsibility for monitoring this policy and holding the headteacher and strategic lead to account for its implementation.

The management committee will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees safeguarding is Phil Healy.

All governors will:

* Ensure that they have read and understand this policy
* Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (appendix 3)
* Meet with nominated member of CELC staff to review every half-term
* Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
* Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The Head of Alternative Provision and Senior Leadership Team are responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school’s DSL’s are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

* Supporting the senior leadership team in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
* Working with the senior leadership team, ICT manager and other staff, as necessary, to address any online safety issues or incidents
* Managing all online safety issues and incidents in line with the school child protection policy
* Ensuring that any online safety incidents are logged along with safeguarding and/or child protection concerns, discussions and decisions in accordance with the CELC Child Protection and Safe-guarding Policy and dealt with appropriately in line with this E-Safety policy.
* Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the CELC Anti-Bullying Policy.
* Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
* Liaising with other agencies and/or external services if necessary
* Providing regular reports on online safety in school to the senior leadership team and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT service

Coventry City Council’s ICT service provide ICT support to the CELC and ensure the following:

* Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
* Monitoring the school’s ICT systems on a regular basis
* Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

* Maintaining an understanding of this policy
* Implementing this policy consistently
* Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet and ensuring that pupils follow the school’s terms on acceptable use.
* Working with the DSL to ensure any online safety incidents are logged along with safeguarding and/or child protection concerns, discussions and decisions in accordance with the CELC Child Protection and Safe-guarding Policy and dealt with appropriately in line with this E-Safety policy.
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
* Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

* Notify a member of staff or the headteacher of any concerns or queries regarding this policy
* Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet (appendices 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

* What are the issues? - [UK Safer Internet Centre](https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues)
* Hot topics - [Childnet International](http://www.childnet.com/parents-and-carers/hot-topics)
* Parent factsheet - [Childnet International](https://www.childnet.com/resources/parents-and-carers-resource-sheet)

3.7 Visitors and members of the community

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

# 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

From September 2020 **all** schools will have to teach:

* [Relationships and sex education and health education](https://schoolleaders.thekeysupport.com/uid/66a1d83e-2fb9-411e-91f1-fe52a09d16d1/) in secondary schools

In **Key Stage 3**, pupils will be taught to:

* Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
* Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

* To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
* How to report a range of concerns

By the **end of secondary school**, they will know:

* Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
* About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
* Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
* What to do and where to get support to report material or manage issues online
* The impact of viewing harmful content
* That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
* That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
* How information and data is generated, collected, shared and used online
* How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
* How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies and workshops to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

# 5. Educating parents about online safety

The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during pupil inductions.

The school will let parents know:

* What systems the school uses to filter and monitor online use
* What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the senior leadership team.

# 6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Key group leaders will discuss cyber-bullying with their key groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

* Poses a risk to staff or pupils, and/or
* Is identified in the school rules as a banned item for which a search can be carried out, and/or
* Is evidence in relation to an offence

Before a search, the authorised staff member will:

* Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
* Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
* Seek the pupil’s cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so.

When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

* Cause harm, and/or
* Undermine the safe environment of the school or disrupt teaching, and/or
* Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / or a member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

* They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
* The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

* **Not** view the image
* Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE’s latest guidance on [screening, searching and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)

Any searching of pupils will be carried out in line with:

* The DfE’s latest guidance on [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation)
* UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)
* Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the school complaints procedure.

# 7. Acceptable use of the internet in school

All pupils are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet.   All staff, governors, volunteers and visitors are expected to adhere to Coventry City Council’s Standard of Acceptable Use of ICT Facilities, Standard for Remote Working and CELC’s Acceptable Use of ICT Facilities in Teaching and Learning.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

# 8. Pupils using mobile devices in school

1. As described within the CELC behaviour policy, at the start of each day, students will be required to hand in their mobile phones and electronic devices.

1. KS3 are required to hand in their phones all day and KS4 will be able to request their phone for use at the beginning of lunchtime.

1. The pupil agreement for Acceptable Use of ICT includes the appropriate use of personal devices at lunchtime.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

# 9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 3.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

* Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
* Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
* Making sure the device locks if left inactive for a period of time
* Not sharing the device among family or friends
* Installing anti-virus and anti-spyware software
* Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the senior leadership team.

# 10. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

# 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

* Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
* Children can abuse their peers online through:
  + Abusive, harassing, and misogynistic messages
  + Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  + Sharing of abusive images and pornography, to those who don’t want to receive such content
* Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

* Develop better awareness to assist in spotting the signs and symptoms of online abuse
* Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
* Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

# 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety through CPOMS.

This policy will be reviewed every year by the SLT with responsibility for safeguarding. At every review, the policy will be shared with the governing board. The review (such as the one available [here](https://360safe.org.uk/)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

# 13. Links with other policies

This online safety policy is linked to our:

* Child protection and safeguarding policy
* Behaviour policy
* Staff disciplinary procedures
* Data protection policy and privacy notices
* Complaints procedure
* ICT and internet acceptable use policy

# Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers)

| Acceptable use of the school’s ICT systems and internet: agreement for pupils and parents/carers | |
| --- | --- |
| **Name of pupil:** | |
| **I will read and follow the rules in the acceptable use agreement policy**  **When I use the school’s ICT systems (like computers) and get onto the internet in school I will:**   * Always use the school’s ICT systems and the internet responsibly and for educational purposes only * Only use them when a teacher is present, or with a teacher’s permission * Keep my username and passwords safe and not share these with others * Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer * Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others * Always log off or shut down a computer when I’m finished working on it   **I will not:**   * Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity * Open any attachments in emails, or follow any links in emails, without first checking with a teacher * Use any inappropriate language when communicating online, including in emails * Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate * Log in to the school’s network using someone else’s details * Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision   **If I bring a personal mobile phone or other personal electronic device into school:**   * I will hand this in upon my arrival at school. * When the phone is in my possession, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online   **I agree that the school will monitor the websites I visit and that there will be consequences if I don’t follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer’s agreement:** I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

# 

# Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

| Acceptable use of the school’s ICT systems and internet: agreement for staff, governors, volunteers and visitors | |
| --- | --- |
| **Name of staff member/governor/volunteer/visitor:** | |
| **When using the school’s ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**   * Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) * Use them in any way which could harm the school’s reputation * Access social networking sites or chat rooms * Use any improper language when communicating online, including in emails or other messaging services * Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network * Share my password with others or log in to the school’s network using someone else’s details * Take photographs of pupils without checking with teachers first * Share confidential information about the school, its pupils or staff, or other members of the community * Access, modify or share data I’m not authorised to access, modify or share * Promote private businesses, unless that business is directly related to the school | |
| I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.  I agree that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.  I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.  I will let the designated safeguarding lead (DSL) and ICT manager (Jesi Dhaliwal) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.  I will always use the school’s ICT systems and internet responsibly and ensure that pupils in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

# Appendix 3: Online safety training needs – self audit for staff

| online safety training needs audit | |
| --- | --- |
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? |  |
| Are you aware of the ways pupils can abuse their peers online? |  |
| Do you know what you must do if a pupil approaches you with a concern or issue? |  |
| Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors? |  |
| Are you familiar with the school’s acceptable use agreement for pupils and parents? |  |
| Do you regularly change your password for accessing the school’s ICT systems? |  |
| Are you familiar with the school’s approach to tackling cyber-bullying? |  |
| Are there any areas of online safety in which you would like training/further training? |  |

# Appendix 4: Online safety incident report log

| online safety incident log | | | | |
| --- | --- | --- | --- | --- |
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |