

Child Protection Framework Policy for Schools

September 2025



This policy was adopted on 7.10.2025

The policy is to be reviewed by 1.9.2026

CONTENTS

1. Contacts
 - School contacts
 - Contacts in the Local Authority
 - Linked policies
 - Definitions
2. Introduction
3. Responsibilities
4. Procedures
5. Record-keeping and retention of records
6. Alternative Provision
7. Confidentiality
8. Recognising abuse
9. Multi-agency working
10. Supporting staff
11. Safer recruitment
12. Allegations against staff, supply staff, volunteers and contractors (including Governors)
13. Whistleblowing
14. Physical intervention/positive handling
15. Anti-bullying
16. Discriminatory incidents
17. Health and Safety
18. Prevention
19. Online safety
20. Sending nude or semi-nude images
21. Child on child abuse, including sexual violence & sexual harassment
22. Cultural Issues
23. So-called 'honour' based abuse
24. Contextual safeguarding and extra familial harm
25. Serious violence
26. Domestic abuse

27. Children in need of a social worker (Child Protection and Child In Need Plans)
28. Mental health
29. Looked After Children
30. Children with family members in prison
31. Homelessness
32. Modern Day Slavery and the National Referral Mechanism
33. Allegations against pupils

APPENDIX A: Terminology

Appendix B: Filtering and Monitoring

1. Contacts

School contacts

Headteacher	Clare Pankhania; headteacher@highworthcombined.co.uk ; 01494 525534
Designated Safeguarding Lead (DSL)	Clare Pankhania; headteacher@highworthcombined.co.uk ; 01494 525534
Deputy Designated Safeguarding Lead(s)	Jillian Armiger; inclusion@highworthcombined.co.uk ; 01494 525534 Brain Stother; deputy@highworthcombined.co.uk ; 01494 525534 Olga Nunn; clarkeo@highworthcombined.co.uk ; 01494 525534 Sarah Cox; coxs@highworthcombined.co.uk ; 01494 525534 Alana Moore; moorea@highworthcombined.co.uk ; 01494 525534
Designated Teacher for Children Looked After (DT for CLA)	Jillian Armiger; inclusion@highworthcombined.co.uk ; 01494 525534
Mental Health Lead	Jillian Armiger; inclusion@highworthcombined.co.uk ; 01494 525534
Prevent Lead	Clare Pankhania; headteacher@highworthcombined.co.uk ; 01494 525534
Nominated Safeguarding Governor	Nicky Bibby; bibbyn@highworthcombined.co.uk ; 01494 525534

Co-Chair of Governors	<p>Saima Ibrahim; ibrahims@highworthcombined.co.uk; 01494 525534</p> <p>Sanam Khan; khans@highworthcombined.co.uk; 01494 525534</p>
------------------------------	--

Contacts in The Local Authority

Education Safeguarding Advisory Service ESAS offers support to education providers to assist them to deliver effectively on all aspects of their safeguarding responsibilities.	01296 387981 Secure-esasduty@buckinghamshire.gov.uk
First Response Team (aka MASH) (including Early Help, Channel) The First Response Team process all new referrals to social care, including children with disabilities. Referrals are assessed by the team to check the seriousness and urgency of the concerns and whether Section 17 and/or Section 47 of the Children Act 1989 apply. The First Response Team will ensure that the referral reaches the appropriate team for assistance in a quick and efficient manner.	01296 383962 Out of hours 0800 999 7677 Secure-cypfirstresponse@buckinghamshire.gov.uk
Local Authority Designated Officer (LADO) The Buckinghamshire Local Authority Designated Officer (LADO) is responsible for overseeing the management of all allegations against people in a position of trust who work with children in Buckinghamshire on either a paid or voluntary basis	01296 382070 Secure-lado@buckinghamshire.gov.uk
Bucks Family Information Service Information for families on a range of issues including childcare, finances, parenting and education	01296 383293
Buckinghamshire Safeguarding Children Partnership (BSCP) Procedures, policies and practice guidelines	

Schools Web School bulletin, Safeguarding links, A-Z guide to information and services	
Thames Valley Police	101 (999 in case of emergency)

This policy should be read in conjunction with the following policies and other policies you feel it would be useful to refer to:

- Anti-bullying
- Attendance
- Behaviour
- Children Looked After
- Complaints
- Equalities
- GDPR
- Lettings
- SEN/Inclusion
- Health & Safety (including managing children with medical needs) & First Aid
- Photography
- E-Safety (including use of mobile/electronic devices)
- Staff Code of Conduct x 2
- PSHE - to include RE & RSE
- Visitors
- Whistleblowing
- Safer Recruitment
- Record Keeping

Definitions

'Safeguarding and promoting the welfare of children is defined for the purpose of this policy as:

- Providing help and support to meet the needs of children as soon as problems emerge
- Protecting children from maltreatment, whether that is in or outside the family home, including online
- Preventing impairment of children's mental and physical health or development
- Ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- Promoting the upbringing of children with their birth parents, or otherwise their family network through a kinship care arrangement, whenever possible and where this is in the best interests of the children
- Taking action to enable all children to have the best outcomes inline with outcomes set out in the Children's Social Care National Framework.

Child protection is part of safeguarding and promoting the welfare of children and is defined for the purpose of this guidance as activity that is undertaken to protect specific children who are suspected to be suffering, or likely to suffer, significant harm. This includes harm that occurs inside or outside the home, including online.'
(*Working Together December 2023*)

Abuse is a form of maltreatment of a child and may involve inflicting harm or failing to act to prevent harm. Further information regarding the categories of abuse can be found in the appendix to this document.

Children includes everyone under the age of 18.

2. Introduction

This policy has been developed in accordance with following legislation and guidance:

- Children Act 1989 (amended 2004)
- “Working Together to Safeguard Children” [Working together to safeguard children - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Working_together_to_safeguard_children.pdf)
- Keeping Children Safe in Education”- statutory guidance for schools and further education colleges - https://assets.publishing.service.gov.uk/media/68add931969253904d155860/Keeping_children_safe_in_education_from_1_September_2025.pdf
- Information Sharing Guidance for Safeguarding Practitioners [Information sharing advice for safeguarding practitioners - GOV.UK](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Information_sharing_advice_for_safeguarding_practitioners.pdf)
- Children Missing Education; Statutory Guidance for Local Authorities - Sept 2016 [Children missing education - GOV.UK](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Children_missing_education.pdf)
- Statutory Guidance issued under section 29 of the Counter-Terrorism and Security Act - 2015 [Prevent Duty Guidance](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Prevent_Duty_Guidance.pdf)
- The Equality Act - 2010 [Equality Act 2010: guidance - GOV.UK](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Equality_Act_2010_guidance.pdf)
- What to do if you’re worried a child is being abused - March 2015 [What to do if you are worried a child is being abused](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/What_to_do_if_you_re_worried_a_child_is_being_abused.pdf)
- Statutory guidance on FGM [Multi-agency Statutory Guidance on Female Genital Mutilation](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Multi-agency_Statutory_Guidance_on_Female_Genital_Mutilation.pdf)

Clear governance and leadership is central to embedding a safeguarding culture. The Governing Body takes its responsibility seriously under **section 175 of the Education Act 2002** to safeguard and promote the welfare of children; working together with other agencies to ensure effective and robust arrangements are in place within our school to identify and support those children who are suffering harm or whom may be at risk of harm.

Maintained schools and pupil referral units insert:

- Section 175 of the [Education Act 2002](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262681/Section_175_of_the_Education_Act_2002.pdf), places a duty on schools and local authorities to safeguard and promote the welfare of pupils

Academies, including free schools, and independent schools insert:

- Part 3 of the schedule to the Education (Independent School Standards) Regulations 2014, which places a duty on academies and independent schools to safeguard and promote the welfare of pupils at the school.

Non-maintained special schools insert:

- Part 1 of the schedule to the Non-Maintained Special Schools (England) Regulations 2015, which places a duty on non-maintained special schools to safeguard and promote the welfare of pupils at the school.

Governors will ensure all staff at the school have read and understood their responsibilities pertaining to **Part 1, Part 5 and Annexe B of Keeping Children Safe in Education**.

All staff are required to read and adhere to the **Staff Code of Conduct**.

Every member of the school community is responsible for contributing to a positive culture of safeguarding.

The school recognises that as well as risks to the welfare of children from within their families, children may be vulnerable to abuse or exploitation from outside their homes, including online and from other children. Staff must remain vigilant and alert to these potential risks.

The aims of this policy are:

To provide an environment in which children feel safe, secure, valued and respected.

To ensure that senior leaders, teaching staff and non-teaching staff, supply staff, governors and volunteers:

- Are aware of the need to safeguard and promote the wellbeing of children
- Identify the need for early support
- Promptly report concerns, in line with guidance from the Buckinghamshire Continuum of Need
- Are trained to recognise signs and indicators of abuse

To provide systematic means of monitoring children known to be or thought to be at risk of harm and ensure contribution to assessments of need and support plans for those children.

To ensure Highworth Combined School and Nursery (HCSN) has a clear system for communicating concerns both internally and with external agencies in line with the Working Together guidance.

To ensure the school has robust systems in place to accurately record safeguarding and child protection concerns.

To develop effective working relationships with all other agencies involved in safeguarding, supporting the needs of children at our school.

To ensure that all staff appointed have been through the safer recruitment process and understand the principles of safer working practices as set out in our **Staff Code of Conduct**.

To ensure that all staff understand the processes in place to manage an allegation against a staff member, governor or volunteer.

To ensure that any community users of our facilities have due regard to expectations of how they should maintain a safe environment, which supports children's wellbeing.

This policy is published on our website, https://www.highworth.bucks.sch.uk/web/child_protection_policy/518697 and hard copies are available from the school office.

3. Responsibilities

All **staff, supply staff, volunteers, visitors, governors and contractors** understand that safeguarding children is everyone's responsibility. Any person who receives a disclosure of abuse, an allegation or suspects that abuse may have occurred must report it immediately to Clare Pankhania, DSL or, in their absence, to Jillian Armiger, Brian Stother, Olga Nunn, Sarah Cox or Alana Moore, Deputy DSL). In the absence of all of the above, concerns will be brought to the attention of the most senior member of staff on site.

Staff must maintain a good working knowledge of the Buckinghamshire Continuum of Need [The Continuum of Need - Buckinghamshire Safeguarding Children Partnership \(buckssafeguarding.org.uk\)](https://www.buckssafeguarding.org.uk) and any updates and how it should be used to inform decision making regarding a referral to First Response.

Staff must have the skills, knowledge and understanding to keep both looked after children and previously looked after children safe.

Staff must understand vulnerability and that barriers exist when recognising abuse. Consider the following groups who may have increased vulnerability:

- Young carers
- Children with SEND
- Children living with domestic abuse
- Children who experiencing poor mental health
- Children whose parents suffer with poor mental health, including substance misuse

- Criminal exploitation, including sexual exploitation, County Lines radicalisation and gang involvement
- Look after children and previously look after children
- Children who have a social worker
- Privately fostered children
- Asylum seekers
- So-called Honour Based Violence, including FGM and forced marriage
- Children who frequently go missing or whose attendance is a concern
- Children who are part of the LGBTQ+ group
- Children who are at risk of discrimination due to faith and belief, race or ethnicity
- Children who have English as an additional language (EAL)
- Children who are living in temporary accommodation.

The Governing Body understands and fulfils its safeguarding responsibilities.

It must:

Ensure that the Headteacher and the DSL(when not the Headteacher) creates and maintains a strong, positive culture of safeguarding within the school.

Ensure that this policy reflects the unique features of the community we serve and the needs of the pupils attending our provision. This policy will be reviewed at least annually and whenever new guidance is issued.

Regularly monitor and evaluate the effectiveness of this Child Protection Policy.

Appoint a Designated Safeguarding Lead (DSL), who is a member of the Senior Leadership Team (SLT) and has the required level of authority and also appoint at least one Deputy DSL. The roles and responsibilities of the DSL and Deputy DSL are made explicit in those post-holders' job descriptions. If not the DSL, the Headteacher still maintains overall responsibility for safeguarding and child protection within the school.

Recognise the importance of the role of the DSL, ensuring they have sufficient time, training, skills and resources to be effective. Refresher training must be attended every 2 years, in addition knowledge and skills must be refreshed at regular intervals, at least annually.

Ensure that all staff complete safeguarding training to include their roles and responsibilities with regards to the school IT system's online filtering and monitoring.

Ensure measures are in place for the governing body to have oversight of how the school's delivery against its safeguarding responsibilities are exercised and evidenced, to include reviewing online filtering and monitoring on a regular basis and at least annually. Ensure robust structures are in place to challenge the Headteacher where there are any identified gaps in practice or procedures are not followed.

Recognise the vital contribution that the school can make in helping children to keep safe, through incorporation of safeguarding within the curriculum. This will also be taught through the PSHE curriculum and relevant issues through the Relationship Education (primary schools) or Relationship Sex Education (secondary schools, mandatory from Sept. 2020). Ensure that through curriculum content and delivery children understand how to keep themselves safe.

Ensure that school is following the statutory RSE guidance –[Relationships and sex education \(RSE\) and health education - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/relationships-and-sex-education-rse-and-health-education)

Ensure safe and effective recruitment policies and disciplinary procedures are in place.

Ensure resources are allocated to meet the needs of pupils requiring child Protection or early intervention.

Ensure the DSL completes an Annual Safeguarding Report for Governors and a copy is shared with the Education Safeguarding Advisory Service at Buckinghamshire Council.

It is the duty of the Co-Chair of Governors, Saima Ibrahim and Sanam Khan to liaise with relevant agencies if any allegations are made against the Headteacher. If there are concerns that issues are not being progressed in an expedient manner, staff/pupils/parents/carers should escalate concerns to the Local Authority Designated Officer (LADO) via First Response.

The Governing body must ensure that procedures are in place to manage, record and escalate as appropriate safeguarding concerns of allegations against staff, supply staff, governors, volunteers, visitors or contractors where they could pose a risk of harm to children. This must include those concerns that do not meet threshold (low-level concerns). The guidance in Part four of [Keeping children safe in education \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671442/Keeping-children-safe-in-education.pdf) must be followed if there were any such concerns.

The Governing Body must ensure that a named teacher is designated for Looked After Children and that an up to date list of children who are subject to a Care Order or are accommodated by the Local Authority is regularly reviewed and updated. The school must work with the Virtual Schools Team to support the educational attainment for those children who are Looked After.

The Governing Body must have assurance that any alternative provision attended by children on roll has appropriate safeguarding arrangements and child protection policies in place. The Governing Body must ensure that any children, at such a provision, are visited whilst they are attending, that the curriculum is appropriate to the needs of the child and that attendance is monitored daily.

Any outside agencies providing services or activities to the school have provided assurances that they have safeguarding policies and procedures in place.

The Governing Body has a statutory duty to appoint a Nominated Governor for safeguarding. The Nominated Governor must be familiar with [Buckinghamshire Safeguarding Children Partnership](#) procedures, Local Authority procedures and guidance issued by the Department for Education. The Nominated Governor must:

- Work with the DSL to produce the Child Protection Policy annually.
- Undertake appropriate safeguarding training, to include Prevent and Safer Recruitment training.
- Ensure child protection is regularly discussed at Governing Body meetings
- Meet at least termly with the DSL to review and monitor the school's delivery on its safeguarding responsibilities, to review the Single Central Record and complete an audit of the staff files
- Ensure that filtering and monitoring systems are in place and take part in the review
- Take responsibility to ensure that the school is meeting the OFSTED requirements as set out in the inspection guidance:

[Education inspection framework \(EIF\) - GOV.UK \(www.gov.uk\)](#)

All governors must complete safeguarding training on appointment, to also include Prevent training. This training must be regularly updated in line with national or local guidance. The governing body must ensure that relevant staff have due regard to the relevant data protection principles set out in the Data Protection Act 2018 and the GDPR, which allow them to share or withhold personal information when it is necessary to safeguard any child.

We have a **Designated Safeguarding Lead (DSL)** who is responsible for:

Creating a culture of safeguarding within the school where children are protected from harm.

Ensuring all staff receive an effective induction and ongoing training to support them to recognise and report any concerns.

Ensuring children receive the right help at the right time using the Buckinghamshire Continuum of Need document.

Ensuring referrals to partner agencies, are followed up in writing, including referrals to First Response and Early Help (FSS).

Establishing and maintaining a safe and secure system for recording safeguarding and child protection records. These records must be audited regularly to ensure all actions are completed.

Ensuring all child protection files are held separately from pupils' educational records.

Maintaining the record for staff safeguarding training.

Ensuring that the safeguarding team contact details and photos are displayed in prominent areas around the school and also on the website.

Being the designated point of contact for staff to be able to discuss and share their concerns.

Ensuring the online filtering and monitoring system is reviewed regularly, at least annually.

Being available to staff and outside agencies during school hours and term time for consultation on safeguarding concerns raised.

Having responsibility to ensure that cover is arranged outside of term-time during working hours, with the expectation that all meetings in school holidays are attended including those convened at short notice.

During residential and extended school hours, ensuring arrangements are in place for staff to have a point of contact.

Contributing effectively to multiagency working, for the safeguarding and promotion of the welfare of children, as set out in Working Together.

Providing the Headteacher (if the Headteacher is not the DSL), with an annual report for the Governing Body, detailing how school delivers on its safeguarding responsibilities and any child protection issues within the school. The Governing Body will use this report to fulfil its responsibility to provide the Local Authority with information about their safeguarding policies and procedures.

Meeting at least once a term with the Nominated Governor to share oversight of the safeguarding provision within the setting, monitor performance and develop plans to rectify any gaps in policy or procedure. A record will be kept of these meetings. Providing the Headteacher (if DSL is not Headteacher) with up to date information of any issues.

Meeting the statutory requirement to keep up to date with knowledge, enabling them to fulfil their role, including attending mandatory and any other additional relevant training.

Referring immediately to the Police, using the guidance, When to call the police [2491596 C&YP schools guides.indd \(npcc.police.uk\)](#) for any cases where a criminal offence may have been committed or risk of harm is imminent.

Completing DSL refresher training every 2 years and updating their skills and knowledge on a regular basis and at least annually, through means such as training, reading bulletins or attending DSL forums.

To fulfil the DSL responsibilities as set out in the KCSIE, Annexe C.

The school's **Headteacher** is responsible for:

Ensuring that this policy is updated annually or before to reflect any changes to guidance and/or legislation.

Ensuring that this policy is published on the school website.

Recording, reviewing and making decisions on any low-level concerns, may be in conjunction with the DSL.

Liaising with the LADO in the event of an allegation being made against a member of the staff, volunteer or an organisation using the school premises.

Liaising with the DSL to ensure they have appropriate time, funding, training and resources to fulfil their role.

Ensuring that appropriate cover is in place to attend strategy meetings or CP conferences that take place during the school holidays or in the event that the DSL is absent.

Ensuring that a designated 'Appropriate Adult' is in place in order to support children in line with the Police and Criminal Evidence (PACE) act, [PACE Code C 2023 \(accessible\) - GOV.UK \(www.gov.uk\)](#) which advises that "The role of the appropriate adult (AA) is to safeguard the rights, entitlements and welfare of juveniles and vulnerable persons", with there being further elaboration that the AA is expected to observe that the police are acting properly and fairly in relation to a vulnerable detained persons rights and entitlements, as well as helping the detained person understand their rights. This can also be found as part the school's Searching and Screening Policy.

4. Procedures

Our school procedures for all staff, supply staff, governors, volunteers, visitors and contractors in safeguarding and protecting children from harm are in line with Buckinghamshire Council and [Buckinghamshire Safeguarding Children Partnership](#) safeguarding procedures, "**Working Together to Safeguard Children**" [Working together to safeguard children - GOV.UK \(www.gov.uk\)](#),

"Keeping Children Safe in Education" [Keeping children safe in education \(publishing.service.gov.uk\)](#) and statutory guidance issued under section 29 of the **Counter-Terrorism and Security Act 2015** [Revised Prevent duty guidance: for England and Wales - GOV.UK \(www.gov.uk\)](#).

We will ensure visitors are:

- Clearly identified with visitor/contractor passes.
- Met and directed by school staff/representatives.

- Signed in and out of the premises by school staff.
- Given a safeguarding leaflet to read or directed to a poster informing them of how to report a concern
- Given restricted access to only specific areas of the school, as appropriate.
- Escorted by a member of staff/representative as required.
- Given access to pupils restricted to the purpose of their visit.

All members of staff must complete safeguarding training every 3 years, attend annual refresher training and partake in any training opportunities arranged or delivered by the DSL. Updates must be cascaded to all staff throughout the year. All new staff will receive safeguarding and child protection training on induction to include online safety and the school's filtering and monitoring system.

All staff will read the Child Protection policy, Part 1 and Part 5 of the KCSIE, at least annually, will sign a declaration to show that the guidance has been reviewed and they have a clear understanding of their role. There are audit methods in place to ensure that staff have understood the content.

All parents/carers must be made aware of the school's responsibilities in regard to child protection procedures through this policy.

All staff, including supply staff, must follow the reporting procedures as follows when reporting any child protection concerns:

- Staff must ensure the child is in a safe place and in receipt of support
- Staff must make a written report using the school record keeping process
- If there is a serious concern and it is close to the end of the school day, staff must make a verbal report to the DSL to alert them to the safeguarding/child protection concern
- Copies of concern forms are handed to supply staff when they arrive at school each day
- Staff must ensure the time and date of the incident is recorded
- A factual account of the incident must be recorded, including who was involved, what was said/seen/heard, where the incident took place and any actual words or phrases used by the child
- Use a body map to record any injuries seen or reported by the child
- Staff must sign and date the report giving details of their role within school
- The DSL must record when the report was passed to them and what action was taken alongside any outcomes achieved. The document will be transferred to Behaviour Watch by the DSL so that an electronic copy is permanently available
- The DSL must ensure the child's wishes and feelings are taken into consideration when deciding on next steps.

Through our **Attendance Policy**, we have a robust system for monitoring attendance which is in line with the latest national attendance guidance, and will act to address absenteeism (including unexplainable and/or persistent absence) with parents/carers and pupils promptly and identify any safeguarding issues arising. We involve the local authority attendance team at appropriate stages.

On the first day of absence, parents or carers must phone the school to leave a message on the answer machine explaining that their child is absent and giving: the child's class; reason for absence and length of absence if known. Alternatively, an email must be sent with the same information to: reception@highworthcombined.co.uk. If a child is absent and we have not heard from a parent or carer, we will phone to ask of the whereabouts of the child. If we are not able to make contact, a home visit may be carried out by a DSL.

All children attending our school are required to have a minimum of two identified emergency contacts. Any pupil whose absence is causing concern and where it has not been possible to make contact with a parent/carer, will be reported as a Child Missing in Education (CME) using the **Buckinghamshire CME Protocol**. Any absence, of a pupil who is currently subject to a child protection or child in need plan is immediately referred to their social worker.

HCSN has a mandatory duty to inform the local authority, via the First Response Team, if they become aware that a child under the age of 16 years is living with someone other than their parent, step-parent, aunt, uncle or grandparent for a period of more than 28 days. This is defined as being a private fostering arrangement.

All staff, parents/carers and children are made aware of the school's complaints and escalation processes, which can be activated in the event of concerns not being resolved after the first point of contact.

Our lettings policy reflects the ongoing responsibility the school has for safeguarding those using the site outside of normal school hours, ensuring the suitability of adults working with children on school sites at any time. School must have sight of the up to date **Child Protection Policy** of any organisation hiring the school's facilities.

The school operates **Safer Recruitment** practices. Governors ensure that staff who are involved in the recruitment process have received safer recruitment training. Robust procedures are in place in order to prevent and deter people who are unsuitable to work with children, from applying or being employed by the school.

Allegations against members of staff, supply staff, governors, including volunteers and contractors are referred to the Local Authority Designated Officer (LADO).

Our procedures are reviewed and updated annually as a minimum, or as there are changes to legislation.

Children are encouraged to share any concerns or worries with staff and are regularly reminded about this as part of the curriculum, assemblies and class register time.

5. Record-Keeping and Retention of Records

When a disclosure of abuse or an allegation against a member of staff or volunteer has been made, no matter how low level, our school must have a record of this. These records are maintained in a way that is confidential and secure, in accordance with our **Record Keeping Policy** and **Data Protection Legislation**.

Records should include:

- a clear and comprehensive summary of the concern
- a clear, detailed and robust chronology must be maintained
- details of how the concern was followed up and resolved
- a note of any action taken, decisions reached and the outcome.

There is a statutory requirement for our school to pass any child protection records to the pupil's next school. This must take place within 5 days of the 1st day of term or within 5 days of an in-year transfer. There must be an auditable system in place to evidence this has taken place. Safeguarding records will be sent separately from the general files using a secure method. No records should be maintained within the school once the files have been transferred.

The last statutory school maintains child protection files until a pupil reaches the age of 25 years, therefore if the transfer school is unknown, or a pupil is going to be electively home educated, any child protection files will remain at our school in a secure location. Child protection files will only be destroyed when the pupil reaches their 25th birthday.

We have a robust system for reviewing our archived information held. Our files are stored and disposed of in line with GDPR protocols, local and national retention policies.

We record low level concerns regarding staff, governors and volunteers and review them regularly to look for patterns, escalation or increase in frequency of concerns and take appropriate action as required.

6. Alternative Provision

When a child is accessing an alternative provision, the school remains responsible for the safeguarding of that child.

HCSN will obtain written information from the alternative provider that appropriate safeguarding checks have been carried out on individuals working at their establishment (i.e. those checks that schools would otherwise perform on their own staff).

HCSN will always know where a child is based during school hours. This includes having records of the address of the alternative provider and any subcontracted provision or satellite sites the child may attend. We will regularly review the alternative provision placements.

Alternative Provision DFE statutory guidance

[Alternative provision - GOV.UK](#)

and

Education for children with health needs who cannot attend school - GOV.UK

(www.gov.uk) – DFE statutory guidance.

[Education for children with health needs who cannot attend school - GOV.UK](#)

7. Confidentiality

We recognise that all matters relating to child protection are confidential. The Headteacher or Designated Safeguarding Lead must only disclose personal information about a pupil to other members of staff on a need to know basis. Staff must not keep duplicate or personal records of child protection concerns. All information must be reported to the Designated Safeguarding Lead and securely stored in the designated location within the school, separate from the pupil records.

All staff are aware they cannot promise a child to keep secrets which might compromise the child's safety or well-being or that of another as they have a duty to share. Staff must, however, reassure the child that information will only be shared with those people who will be able to help them and therefore need to know.

We will always undertake to share our intention to refer a child to Social Care (First Response) with their parent/carer's consent, unless to do so could put the child at greater risk of harm or impede a criminal investigation. If in doubt, we will consult with First Response on this point. We recognise that GDPR data Protection Act 2018 must not be a barrier for sharing information regarding safeguarding concerns in line with **'Working Together'**. Gov guidance link:

<https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>

8. Recognising abuse

In the event of a child disclosing abuse staff must:

Refer to the following guidance:

"What to do if You're Worried a Child is Being Abused"

[Stat guidance template \(\[publishing.service.gov.uk\]\(http://publishing.service.gov.uk\)\)](#)

Listen to the child, allowing the child to tell you what has happened in their own way and at their own pace. Staff must not interrupt a child who is freely recalling significant events. Remain calm. Be reassuring and supportive, endeavouring not to respond emotionally.

Do not ask leading questions. Staff are reminded to ask questions only when seeking clarification about something the child may have said or to gain sufficient information to know that this is a safeguarding concern. Staff are trained to use TED; Tell, Explain, Describe.

Make an accurate record of what they have seen/heard using the school's record keeping processes, recording; times, dates or locations mentioned, using as many words and expressions used by the child, as possible. Staff must not substitute anatomically correct names for body part names used by the child.

Reassure the child that they did the right thing in telling someone.

Staff must explain to the child what will happen next and the need for the information to be shared with the DSL.

In the unlikely event the DSL and the deputy DSL are not available, staff are aware they must share their concerns with the most senior member of staff.

If there is immediate risk of harm to a child, staff will NOT DELAY and will ring 999.

The child will be monitored/accompanied at all times following a disclosure, until a plan is agreed as to how best they can be safeguarded.

Reporting systems for children:

At HCSN children are made to feel safe and secure to share any concerns that they may have and know the systems in place for making any such report.

Following a report of concerns the DSL must:

Decide whether there are sufficient grounds for suspecting significant harm, in which case a referral must be made to First Response and the police if it is appropriate, referring to the guidance, When To Call The Police:

[when-to-call-the-police--guidance-for-schools-and-colleges.pdf \(npcc.police.uk\)](#)

The rationale for this decision should be recorded by the DSL.

School must try to discuss any concerns about a child's welfare with parents/carers and, where possible, obtain informed consent before making a referral to First Response. However, in accordance with DfE guidance, this should only be done when it will not place the child at increased risk or could impact a police investigation. Where there are doubts or reservations about involving the child's family, the DSL should clarify with First Response or the police whether the parents/carers should be told about the referral and, if so, when and by whom. This is important in cases where the police may need to conduct a criminal investigation. The child's views must also be taken into account.

If there are grounds to suspect a child is suffering or is likely to suffer significant harm, the DSL (or Deputy) must contact First Response by telephone immediately, in first instance and then complete the Multi Agency Referral Form (MARF).

If the child is in immediate danger and urgent protective action is required, the police and/or ambulance must be called, via 999. The DSL must notify First Response of the occurrence, what action has been taken and to take advice about informing parents/carers.

9. Multi-agency working

HCSN know what the role of schools is, as a relevant agency, within the three safeguarding partner arrangements and as required, will contribute to multi-agency working, in line with the statutory guidance 'Working Together to Safeguard Children'.

When named as a relevant agency and involved in safeguarding arrangements, HCSN will co-operate alongside other agencies with the published arrangements.

HCSN will contribute to inter-agency plans to offer children support of early help and those children supported through child protection plans.

HCSN will allow access for and work with children's social care to conduct or consider whether to conduct as section 17 or section 47 assessment.

If, following a referral, the situation is not improving for the child, the DSL will follow the escalation process.

10. Supporting Staff

We recognise that staff becoming involved with a child who has suffered harm, or appears to be likely to suffer harm, could find the situation stressful and upsetting. We will support such staff by providing an opportunity to talk through their anxieties with the DSL and to seek further support if necessary. This could be provided by the Headteacher or another trusted colleague, Occupational Health, and/or a representative of a professional body or trade union as appropriate.

11. Safer Recruitment

HCSN follows the guidance as set out in the KCSIE together with the information provided by the Bucks Safeguarding Children Partnership to ensure that all the appropriate checks have been carried out on new staff and volunteers.

[Safer Employment & the LADO \(Allegations\) - Buckinghamshire Safeguarding Children Partnership \(buckssafeguarding.org.uk\)](https://www.buckssafeguarding.org.uk)

12. Allegations against staff, supply staff, volunteers and contractors (including Governors)

Here at HCSN, we have our own procedures for managing concerns and/or allegations against those working in school to include staff, supply teachers, volunteers and contractors.

KCSIE date removed - Part four contains comprehensive guidance covering the two levels of allegations/concern:

1. allegations that may meet the harms threshold
2. Allegations/concerns that do not meet the harms threshold - referred to for the purpose of this guidance as 'low level concerns'.

All school staff, supply staff, volunteers and contractors must take care not to place themselves in a vulnerable position with a child. It is always advisable for interviews or work with individual children or parents/carers to be conducted in view of other adults.

We understand that a pupil may make an allegation against a member of staff, member of supply staff, volunteer or contractor. If such an allegation is made, the member of staff notified of the allegation will immediately inform the Headteacher or the most senior teacher if the Headteacher is not present. If the allegation is made against the Headteacher, the Chair of Governors must be informed.

At HCSN we recognise that an allegation may be made if a member of staff, a member of supply staff, a governor, a volunteer or a contractor has:

- Behaved in a way that has harmed a child, or may have harmed a child
- Possibly committed a criminal offence against or related to a child
- Behaved towards a child or children in a way that indicates he or she may pose a risk of harm to children
- Behaved or may have behaved in a way that indicates they may not be suitable to work with children. This includes behaviours both inside and outside of school.

The Headteacher/Senior Teacher/Chair of governors (where the allegation is in reference to the Head Teacher) on all such occasions must immediately discuss the content of the allegation with the Local Authority Designated Officer (LADO).

The Head Teacher/Senior Teacher/ Chair of Governors must:

Follow all advice given by the LADO throughout the investigation process, including how to manage the staff member, supply staff member, governor, volunteer or contractor against whom the allegation is made, as well as supporting other staff, supply staff members, governors, volunteers and contractors within the workplace.

Follow all advice given by the LADO relating to supporting the child making the allegation, as well as other children connected to the organisation.

Ensure feedback is provided to the LADO about the outcome of any internal investigations.

The school will follow the local safeguarding procedures for managing allegations against staff, supply staff, governors, volunteers and contractors, a copy of which can be found in the staff room and on the schools electronic information system.

If the allegation is made against a member of staff supplied by an external agency, the agency will be kept fully informed and involved in any enquiries from the LADO.

Suspension of the member of staff against whom an allegation has been made needs careful consideration and, if necessary, we will consult with the LADO in making this decision. Guidance will also be sought from HR.

Our lettings agreement for other users requires that the organiser will follow the Buckinghamshire Council procedures for managing allegations against staff and where necessary, the suspension of adults from school premises.

Should an individual staff member, supply staff member, governor, volunteer or contractor be involved in child protection, other safeguarding procedures or Police investigations in relation to abuse or neglect, they must immediately inform the Head Teacher. In these circumstances, the school will need to assess whether there is any potential for risk of transfer to the workplace and the individual's own work with children.

Where there are low level concerns recorded against a member of staff, these should be reviewed regularly, and if they are considered significant, the processes for allegations should be followed.

13. Whistleblowing

We have a **Whistleblowing Policy** which can be found in the school's electronic information system. Staff are required to familiarise themselves with this document during their induction period.

All staff must be aware of their duty to raise concerns about unsafe practice or the attitude or actions of colleagues and report their concerns to the Headteacher or Chair of Governors.

Low-level concerns

At HCSN all staff know they have a responsibility to share any concerns, no matter how small, about any adults working in school to any of the DSLs using the Behaviour Watch electronic records system. Staff are made aware of what a low-level concern might look like using the examples from the KCSIE page 10. All reports will be dealt with effectively and recorded, enabling the school to identify any concerning behaviour and support any adults becoming the subject of false low-level concerns.

14. Physical intervention/Positive handling

Our policy on physical intervention/positive handling by staff is set out separately, as part of our **Use of Reasonable Force Policy** and follows the government guidance.

[Use of reasonable force in schools - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

15. Anti-Bullying

Anti-Bullying is referenced within the **Anti-Bullying Policy** and measures are in place to prevent and respond to all forms of bullying, which acknowledges that to allow or condone bullying may lead to consideration under child protection procedures.

16. Discriminatory Incidents

In line with the **Equalities Act 2010**, our **Equalities Policy** addresses all forms of discriminatory incidents.

17. Health and Safety

We recognise the importance of safeguarding pupils throughout the school day. Our **Health and Safety policy** reflects the consideration we give to the protection of our children, both physically and emotionally, within the school environment.

Part of the safeguarding measures we have in place include the safe drop off and collection of pupils at the start and end of the school day as follows:

For pupils in years Nursery to Year 3:

- Pupils must be dropped off and collected by someone over 16
- Pupils must be taken to the relevant entrance for their class
- Pupils must be collected from the relevant entrance and will be handed over from the teacher to the adult
- If a pupil is to be collected by anyone not a parent or carer, the school must be notified in advance. If no notification has been received, a phone call will be made to check arrangements before the pupil is allowed to leave

For pupils in Years 4 to 6:

All of the above apply, unless a letter has been sent to the class teacher giving permission for the pupil to arrive and leave school without adult supervision

Pupils who leave the site during the school day do so only with the written permission of a parent/carers and are collected by an authorised adult. School must be notified by the parents/carers regarding whom they have authorised for this task.

In the event of a pupil going missing during the course of the school day we will carry out immediate checks to ensure the pupil is not on site, we will then make contact with the pupil's parents/carers and inform the police.

When the school is hired out to a 3rd party provider, we ensure that they have appropriate arrangements in place to keep children safe through the sight of their child protection and safer recruitment procedures.

At HCSN we ensure that we are aware of the content of materials used by any visiting speakers prior to their visit.

18. Prevent Duty

We are aware of the Prevent Duty under **Section 26 of the Counter Terrorism and Security Act 2015** to protect young people from being drawn into terrorism.

All school staff and governors have completed Prevent training and we have training logs to evidence this.

We have in place and monitor appropriate web filtering systems.

The DSLs and senior leaders are familiar with their duties under The Prevent Duty Guidance: [Revised Prevent duty guidance: for England and Wales - GOV.UK](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/616222/Revised_Prevent_duty_guidance_for_England_and_Wales.pdf) (www.gov.uk)

19. Online Safety

All staff are aware of the school policy for **Online-Safety** which sets out our expectations relating to:

- Creating a safer online learning environment,
- Giving everyone the skills, knowledge and understanding to help children stay safe on-line, question the information they are accessing and support the development of critical thinking,
- Inspiring safe and responsible use of mobile technologies, to combat behaviours on-line which may make pupils vulnerable, including the sending of nude or semi-nude images.
- Use of camera equipment, including smart phones.
- What steps to take if there are concerns and where to go for help.
- Staff use of social media as set out in the **Staff Code of Conduct**.

Cyber-bullying by children, via texts, social media and emails, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

School are aware of the risks posed by children in the online world; in particular non-age appropriate content linked to self-harm, suicide, grooming and radicalisation.

Pupils, staff and parents/carers are supported to understand the risks posed by:

- the CONTENT accessed by pupils – risks such as misinformation, disinformation, including fake news and conspiracy theories.
- their CONDUCT on-line
- who they have CONTACT within the digital world
- COMMERCE - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

HCSN has online filtering and monitoring systems in place to ensure children are safeguarded from potentially harmful online material. These systems are regularly monitored, at least annually, by the DSL, IT provider and nominated governor. A record will be kept of the reviews.

School will follow the advice as given by the government, to advise and support children with any online learning taking place at home to ensure this is done so safely.

We have a separate **Mobile Phone Policy** which sets out the acceptable use of mobile technologies by pupils whilst onsite. This includes sanctions which will be applied when these boundaries are not adhered to.

Visitors to our school are respectfully requested to turn all mobile devices off.

Staff use of mobile technology whilst on site is set out in the **Staff Code of Conduct**.

All staff receive online awareness training in order to understand the risks children are exposed to. On induction and at least once per academic year.

All staff have an understanding of expectations roles and responsibilities with regards to the online filtering and monitoring processes.

The DfE has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.

[Generative AI: product safety expectations - GOV.UK](#)

20. Sending nude or semi-nude images

Sending nude images or semi-nude images, is one of a number of ‘risk-taking’ behaviours associated with the use of digital technologies, social media or the internet. It is accepted that children experiment and challenge boundaries and therefore the risks associated with ‘online’ activity can never be completely eliminated.

Further advice and guidance can be found using the link below:

[Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](#)

Staff, pupils and parents/carers are supported, via training, to understand the creation and sharing of sexual imagery, such as photos or videos, of under 18s is illegal. This includes images of pupils themselves if they are under the age of 18.

Any disclosures/incidents that occur will follow the normal safeguarding practices and protocols for our school. We will also use the guidelines for responding to incidents, as set out in:

[Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)

produced by the UK Council for Internet Safety. The DSL will inform parents/carers of any incidents.

21. Child on Child Abuse, including sexual violence and sexual harassment.

HCSN believes that all children have a right to attend school and learn in a safe environment free from harm by both adults and other pupils. We recognise that some safeguarding concerns can occur via child on child abuse.

All staff operate a zero-tolerance policy to child on child abuse and will not pass off incidents as 'banter' or 'just growing up'.

All staff recognise that child on child issues may include, but may not be limited to:

- Bullying (including cyber bullying)
- Racial abuse
- Physical abuse, such as hitting, hair-pulling, shaking, biting or other forms of physical harm
- Sexual violence and sexual harassment
- Causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party (Harmful sexual behaviour HSB)
- Abuse related to sexual orientation or identity
- Sending nude or semi-nude images (consensual & non-consensual)
- Upskirting and initiation/hazing type violence and rituals
- Emotional abuse
- Abuse within intimate partner relationships

All staff should be able to reassure victims that they are being taken seriously and that they will be supported and kept safe. Incidents of child on child abuse must be reported to the DSL, who will refer to the appropriate agencies as required.

The following will be considered when dealing with incidents:

- Whether there is a large difference in power between the victim and perpetrator i.e. size, age, ability, perceived social status or vulnerabilities, including SEND, CP/CIN or CLA

- Whether the perpetrator has previously tried to harm or intimidate pupils
- Any concerns about the intentions of the alleged perpetrator
- How to best support and protect the victim and alleged perpetrator as well as any other children who may have been involved or impacted.
- Risk assessments and safety planning will be created in conjunction with external professionals.

In order to minimise the risk of child on child abuse taking place, as a school we must:

- Deliver RE/RSE/PSHE to include teaching pupils about how to keep safe and understanding what acceptable behaviour looks like
- Ensure that pupils know that all members of staff will listen to them if they have concerns and will act upon them
- Have systems in place for any pupil to be able to voice concerns
- Develop robust risk assessments if appropriate
- Refer to any other relevant policies when dealing with incidents, such as the **Behaviour Policy** and/or the **Anti-Bullying Policy**.

We recognise that 'Upskirting' involves taking a photograph under an individual's clothing without their knowledge. We understand that it causes the victim distress and humiliation and that any gender can be a victim. Staff recognise that 'Upskirting' is a criminal offence and must promptly report any such incidents to the Headteacher, DSL or most senior member of staff.

Reference will be made to the following government guidance and part 5 of the **Keeping Children Safe in Education** to ensure that all staff have an understanding of the serious nature of sexual violence and sexual harassment between children in schools. The school ensure that they keep up with current legislation and practice referring to trusted advisors such as BSCP, NSPCC and Ofsted guidance.

Sexual violence and sexual harassment can occur between two children of **any age and sex**. It can occur through a group of children sexually assaulting or sexually harassing a single child or group of children. This can occur online, face to face (both physically and verbally) and can take place inside or outside of school. As set out in Part five of the KCSIE, all staff maintain an attitude of '**it could happen here**' and it is never acceptable.

All staff have a responsibility to address inappropriate behaviour in a timely manner, however seemingly insignificant it may appear.

All victims will be reassured that they are being taken seriously and that they will be supported and kept safe. No child will ever be made to feel ashamed for making a report or that they are creating a problem for our school.

Support will be given to both victims and perpetrators as required.

22. Cultural Issues

As a school we are aware of the cultural diversity of the community around us and work sensitively to address the unique culture of our pupils and their families as they relate to safeguarding and child protection. This includes children at risk of harm from abuse arising from culture, ethnicity, faith and belief on the part of their parent, carer or wider community.

Staff must report concerns about abuse linked to culture, faith and beliefs in the same way as other child protection concerns.

23. So-Called 'Honour' Based Abuse

Staff at our school understand there is a legal duty to report known cases of Female Genital Mutilation (FGM) and So Called 'Honour' Based Abuse to the police and they will do this with the support of the DSL. [Mandatory reporting of female genital mutilation: procedural information - GOV.UK](#)

Our school is aware of the need to respond to concerns relating to forced marriage and understand that it is illegal, a form of child abuse and a breach of children's rights. We recognise some pupils, due to capacity or additional learning needs, may not be able to give an informed consent and this will be dealt with under our child protection processes. HCSN staff can contact the Forced Marriage Unit if they need advice or information. Contact 020 7008 0151 fm@fcdo.gov.uk

We are aware of the signs of FGM [Female genital mutilation \(FGM\) | NSPCC](#)

We recognise both male and female pupils may be subject to honour-based abuse.

We promote awareness through training and access to resources, ensuring that the signs and indicators are known and recognised by staff.

Any suspicions or concerns for forced marriage are reported to the DSL who will refer to First Response or the police if emergency action is required.

24. Contextual Safeguarding and extra-familial harms

Contextual Safeguarding is an approach to understanding and responding to children's experiences of significant harm beyond their families. Extra-familial harm is linked to contextual safeguarding; these concepts refer to harms that occur outside of the family system, including harmful online contact.

At HCSN all staff recognise that pupils may encounter safeguarding incidents that happen outside of school and can occur between children outside of this environment. We will respond to such concerns, reporting to the appropriate agencies in order to support and protect the pupil.

All staff and especially the DSLs, will consider the context of incidents that occur outside of school to establish if situations outside of their families may be putting the

pupil's welfare and safety at risk of abuse or exploitation, including (but not limited to) sexual exploitation, criminal exploitation and serious youth violence.

Children who may be alleged perpetrators will also be supported to understand the impact of contextual issues on their safety and welfare.

In such cases the individual needs and vulnerabilities of each child will be considered.

Further guidance can be found at: <https://contextualsafeguarding.org.uk/>

25. Serious Violence

All staff are aware of signs and indicators which may signal that children are at risk from, or are involved with, serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or significant change in well-being or signs of assault or unexplained injuries. Staff are aware that unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs.

At HCSN we are aware of the range of risk factors which increase the likelihood of involvement in serious violence such as being male, having been frequently absent or permanently excluded from school, having experienced child maltreatment and having been involved in offending such as theft or robbery. School will take appropriate measures to manage any situations arising. [Preventing youth violence and gang involvement - Practical advice for schools and colleges \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61422/preventing-youth-violence-and-gang-involvement-practical-advice-for-schools-and-colleges.pdf)

26. Domestic Abuse

All staff recognise that children who experience domestic abuse, including intimate partner abuse, referred to as 'teenage relationship abuse' KCSIE, can suffer long lasting emotional and psychological effects. Staff also recognise the impact on children seeing, hearing or experiencing the effects of domestic abuse. Staff must report any concerns using the school's safeguarding procedures.

27. Children who need a social worker (Child Protection and Child In Need Plans)

Staff recognise that children may have a social worker due to safeguarding or welfare needs and this can cause them to have barriers with attendance, behaviour, learning and mental health. HCSN will share information with a social worker for any child whom they are supporting to ensure decisions are made in the best interests

of the child. Informed decisions, will be made by staff with regards to safeguarding for those children who are being supported by a social worker.

The Virtual School lead the support for this cohort of children and HCSN will work in partnership with them and the Local Authority to improve outcomes for these children.

28. Mental Health

At HCSN, we are aware that mental health problems can be an indicator that a child has suffered or may be at risk of suffering abuse, neglect, or exploitation.

Staff recognise that traumatic adverse childhood experiences can have lasting impact throughout a child's life and this can impact on mental health, behaviour and education.

Staff will report any mental health concern that is linked to a safeguarding concern to the DSL.

Where there are concerns for a child's mental health HCSN will seek advice from a trained professional, who would be able to make a diagnosis of a mental health problem.

[Mental health and behaviour in schools \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

29. Looked After Children

HCSN has a named Designated Teacher (DT), who is responsible for promoting the education achievement and well-being for LAC and previously LAC children.

The DT works closely with the DSL to ensure that any safeguarding concerns are responded to quickly and effectively and are shared with the appropriate agencies.

The Virtual School, who is responsible for overseeing the progress of this group of children, work in partnership with the DT and other agencies, supporting them to promote better outcomes for these children.

30.Children with family members in prison

Children who have a parent in prison are at risk of poor outcomes including poverty, stigma, isolation and poor mental health. School will access support for any affected children through The National Information Centre on Children of Offenders (NICCO) who can provide information designed to support professionals working with offenders and their children. [NICCO](https://www.nicco.org.uk/)

31. Homelessness

HCSN recognises that being homeless or being at risk of becoming homeless presents a real risk to a child's welfare and that some 16 and 17 year olds could be living independently from their parents or guardians. If there are indicators that a family or individual are at risk, school will seek timely support from the local authority.

32. Modern Slavery and the National referral Mechanism

Modern slavery encompasses human trafficking and slavery, servitude and forced or compulsory labour. Exploitation can take many forms, including sexual exploitation, forced labour, slavery, servitude, forced criminality and the removal of organs. If school are concerned that a child is being affected by modern slavery they will refer to the home office guidance for further information on the indicators that someone may be a victim, what support is available to victims and how to refer them to the NRM, whilst also seeking support from the local authority.

[Modern slavery: how to identify and support victims - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/modern-slavery-how-to-identify-and-support-victims)

33. Allegations against pupils

If an allegation is made against a pupil, the school will follow the procedures in the Behaviour Policy with regards to sanctions that may need to be applied.

Where there is a risk of significant harm, a child on child referral will be made to Children's Services for either victim, perpetrator or both.

If it is necessary for a child to be interviewed by the police, or other authorities, school will ensure that parents/carers are informed as soon as possible, following advice from external agencies and that the child is supported by an appropriate adult during the interview. The safety and welfare of the child will always be carefully considered by school.

Appendix A

Everyone who works with children has a duty to safeguard and promote their welfare. They should be aware of the signs and indicators of abuse and know what to do and to whom to speak if they become concerned about a child or if a child discloses to them.

The following is intended as a reference for school staff and parents/carers if they become concerned that a child is suffering or likely to suffer significant harm.

The Children Act 1989 defines abuse as when a child is suffering or is likely to suffer 'significant harm'. Harm means ill treatment or the impairment of health or development. Four categories of abuse are identified:

Categories of Abuse

Child abuse is a form of maltreatment. Somebody may abuse or neglect a child by inflicting harm, or by failing to act to prevent harm. Children people may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults, or another child or children.

Physical Abuse

A form of abuse which may involve; hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating, or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illness in a child.

Emotional Abuse

The persistent emotional maltreatment of a child such as to cause severe and persistent adverse effects on the child's emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child's developmental capability, as well as overprotection and limitation of exploration and learning, or preventing the child participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyber bullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of

emotional abuse is involved in all types of maltreatment of a child, though it may occur alone.

Sexual Abuse

Involves forcing or enticing a child to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.

Neglect

The persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to:

- a) provide adequate food, clothing and shelter (including exclusion from home or abandonment)
- b) protect a child from physical and emotional harm or danger
- c) ensure adequate supervision (including the use of inadequate caregivers)
- d) ensure access to appropriate medical care or treatment. It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

Exploitation

Exploitation is a form of child abuse and may take a number of forms:

Child Sexual Exploitation (CSE) and child Criminal Exploitation (CCE)

Both CSE and CCE are forms of abuse that occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into taking part in sexual or criminal activity, in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of the perpetrator or facilitator and/or through violence or the threat of violence. CSE and CCE can affect children, both male and female and can include children who have been moved (commonly referred to as trafficking) for the purpose of exploitation.

Taken from – **Keeping Children Safe in Education.**

[Home Office – Serious Violence Strategy, April 2018 \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672872/Keeping_Children_Safe_in_Education.pdf)

County Lines

County lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs using dedicated mobile phone lines or other form of “deal line”. This activity can happen locally as well as across the UK - no specified distance of travel is required. Children and vulnerable adults are exploited to move, store and sell drugs and money. Offenders will often use coercion, intimidation, violence (including sexual violence) and weapons to ensure compliance of victims. Taken from “**Keeping Children Safe in Education**”

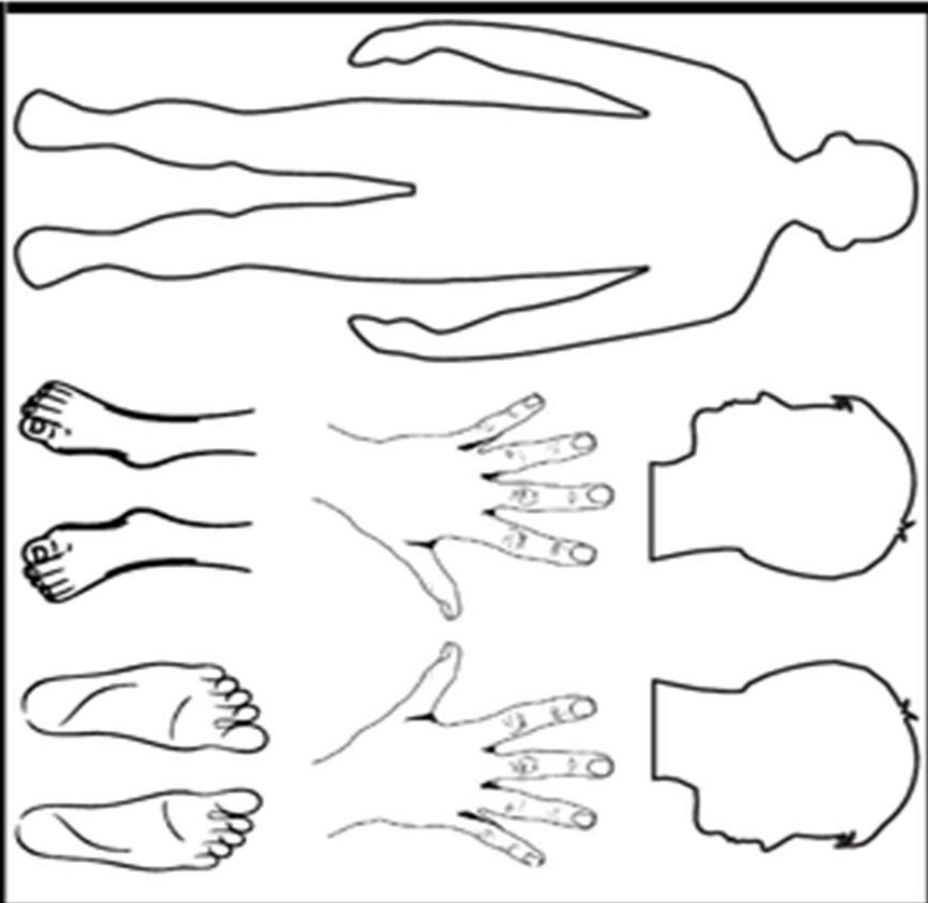
Extremism

Extremism is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces. Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Harmful sexual behaviour (HSB)

Children’s sexual behaviour ranges, from normal and developmental expected to inappropriate, problematic, abusive and violent. The inappropriate, problematic, abusive and violent behaviour can cause developmental damage and is referred to as “Harmful Sexual Behaviour” (HSB).

CHILD PROTECTION BODY MAP



Name of child:

.....

Date of birth:

.....

Staff member raising concern:

.....

Date recorded:

.....

Observations:

.....

.....

.....



Appropriate Filtering for Education settings

May 2023

Filtering Provider Checklist Responses

Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”. Furthermore, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”. There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.



The Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness” and they “should be doing all that they reasonably can to limit children’s exposure to [Content, Contact, Conduct, Contract] risks from the school’s or college’s IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined ‘appropriate filtering standards’. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Securly
Address	Third Floor One London Square, Cross Lanes, Guildford, Surrey, United Kingdom, GU1 1UN https://www.securly.com/
Contact details	uksales@securly.com 0141 343 8322
Filtering System	Securly Filter and Aware
Date of assessment	3rd August 2023

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
<ul style="list-style-type: none"> Are IWF members 		Securly is a current member of the Internet Watch Foundation and has been since 01/03/2016.
<ul style="list-style-type: none"> and block access to illegal Child Abuse Images (by actively implementing the IWF URL list) 		All Securly customers are blocked access to the IWF CAIC list of domains and URLs which host illegal child abuse content.
<ul style="list-style-type: none"> Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' 		Securly integrates and blocks unlawful terrorist content using the list provided by the UK Home Office and Met Police CTIRU (Counter-Terrorism Internet Referral Unit).
<ul style="list-style-type: none"> Confirm that filters for illegal content cannot be disabled by the school 		Securly Filter cannot be disabled by the school. All illegal content categories are locked at a system level. Schools cannot disable these filters.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Securly provides a "Hate" category which allows administrators to block access and alert on websites and content which promote hatred and discrimination across race, religion, age, or sex.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Securly provides a "Drugs" category which allows administrators to block access and alert on websites and content which includes details of manufacture, sale, distribution, and recreational use of illegal substances.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Securly includes the Home Office / Met Police CTIRU illegal terrorist content blocklist and provide a "Hate" category. This allows administrators to block access and alert on websites and content which promotes terrorist organisations and actions, violence, and intolerance.
Gambling	Enables gambling		Securly provides a "Gambling" category which allows administrators to block access and alert on websites and content that promotes betting or risky actions for a reward.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Securly provides a "Network Misuse" category which allows administrators to block access and alert on websites such as VPNs, the Tor network, known malware hosts, C&C servers, and anonymous proxy servers which would allow bypass of filtering or potential harm to a school network.

Pornography	displays sexual acts or explicit images		Securly provides a "Pornography" category which allows administrators to block access and alert on websites that display sexual acts or explicit images.
Piracy and copyright theft	includes illegal provision of copyrighted material		<p>Securly provides a "Streaming Media" category to restrict access to streaming media providers.</p> <p>The "Network Misuse" category will restrict access to common filesharing platforms.</p> <p>Enforced "Creative Commons" mode can be enabled for image search to limit results to only those available under the Creative Commons license.</p>
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		<p>Securly Aware uses AI sentiment analysis to detect self-harm content, emails, web searches and social media posts.</p> <p>Alerts are categorised under the terms 'Self-harm' and 'Grief'</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>
Violence	Displays or promotes the use of physical force intended to hurt or kill		<p>Securly Filter and Aware uses AI sentiment analysis to detect violent content, emails, web searches and social media posts.</p> <p>Alerts are categorised under the terms 'Violence'</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

- Audit logs. Keeps a record of each instance when an admin or teacher allows a site.
- Securly Filter categories include keywords/phrases, URLs and domains of over the top one million websites globally and growing.
- Securly PageScan, using AI and human moderation, provides automated categorisation of previously unknown websites by scanning page content and images.
- Selective HTTPS man-in-the-middle decryption provides real-time dynamic URL filtering, keyword filtering and sentiment analysis.
- Our customers can provide their own block and allow lists in policies and can submit any websites for inclusion in our categories.
- Securly can transparently proxy select websites on demand, allowing us to detect cyberbullying, suicide, and violence, on social media websites such while providing fast URL filtering on the rest of the traffic—on any device, anywhere.
- Take-home policies. Devices that go home can easily have separate policies based on location, rather than time-based roles – these policies automatically change when the device is back on a school network.
- Delegated admins can control policies that are associated with the pupils they have visibility of, ideal for multi-academy trusts who want to give control out to schools whilst maintaining overall management.
- With Securly Home (an add-on for Filter) parents can view their child's recent searches, sites visited, and videos watched on their school-owned device depending on the level of control set by the school.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

All customer log data is stored securely within Securly's servers for a minimum of 1 year as standard. Customers can discuss their individual retention requirements if this is unsuitable.

Activity logs are stored in AWS EU-West-2 (London). There is some processing done on EU-West-1 (Dublin) for the dashboard and any scheduled reports. Our support team is around the world and may access your data as part of a support ticket, but it will remain in the UK.

To ensure the ongoing availability of critical data, management has established a schedule of backups and data redundancy. Backups and replications are monitored for failures, and resolved in a timely manner.

Securly has achieved SOC2 Type 2 certification, demonstrating a commitment to data security and responsibility.

Backups of production databases are performed based on the database type:

- Configuration - daily full snapshots/AMI backups and retained for 7 days
- Logs - monthly backups retained for one month.
- Data is replicated across geographically separate availability zones.
- Backups and replications are monitored for failures. In the event of three successive nightly failures, IT will open an incident ticket to investigate the issue.
- IT performs restorations of data per customer or business requests. System restore capabilities are tested at least annually.

[How Does Securly Comply with GDPR?](#) For information about GDPR or if you have any questions about our GDPR compliance, please contact us at support@securly.com

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Unlike traditional on-premise filtering solutions, Securly will selectively intercept web traffic to block and filter content. This prevents over blocking or problems accessing safe content and education applications.

Previously unknown or uncategorised websites will be analysed by Securly PageScan to accurately determine their category and if they need to be filtered.

Administrators also have ability to manage their own safe sites and override Securly categorised websites.

[How does temporarily allow sites work?](#)

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff 		<p>Securly Filter is built exclusively for education and has school appropriate filtering configured out-of-the-box and allows easy configuration of more strict or relaxed policies as required.</p> <p>Securly Filter includes the ability to generate instant alerts for blocked content. This is configurable at a policy level to allow for different alert levels for vulnerable users.</p> <p>Securly can be configured to define separate filtering policies appropriate to different age groups or roles. E.g. Staff, Primary School Students, Senior Students, Criminology Students, etc.</p>
<ul style="list-style-type: none"> Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS. 		<p>Securly works with schools to ensure Securly Filter is applied in the most robust way possible and includes publicly available best practice guides and recommendations for configuring devices and networks to best protect children and prevent circumvention.</p> <p>Securly provides a “Network Misuse” category to prevent access to websites that provide proxy circumvention services or VPNs.</p> <p>Securly publishes best practice guidance on how to help prevent circumvention.</p> <p>Securly MDM and Classroom can help restrict access to applications, and allows teachers to monitor student devices.</p>
<ul style="list-style-type: none"> Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes 		<p>Securly administrators can permit or deny access to content by using their own domain names and keywords globally or per policy.</p> <p>Staff members assigned to Faculty Groups can edit policies that affect OUs or Security Groups assigned to them. This feature can be enabled and disabled at an admin level.</p>

		Any substantial changes to the system are logged in an audit trail.
<ul style="list-style-type: none"> Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter. 		<p>Securly Filter and it's classification engine PageScan looks at content of new sites to determine an appropriate category. For sites that have little or no metadata to interrogate, Securly PageScan processes images within a site and will classify as Pornography if ANY of the images are perceived to contain nudity, this is an automated process.</p> <p>Securly can filter SSL traffic, providing full protection and customisation as necessary, while only decrypting websites under our blocked categories, leaving other sites alone. This helps eliminate latency, and allow full scalability while taking care of HTTPS traffic.</p> <p>Securly Aware is able to monitor chat logs and posts that are submitted to selected sites, such as ChatGPT, TikTok, Twitter, Facebook, Instagram.</p>
<ul style="list-style-type: none"> Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking 		<p>Securly publishes details of its filtering approach and rationale on the publicly available knowledgebase.</p> <p>More information on Securly PageScan technology can also be found on our tech blog.</p>

<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>As a cloud-based service, Securly Filter and Aware are available anywhere with Internet access.</p> <p>Delegated control can be provided to additional administrators or Safeguarding teams.</p> <p>Multiple sites and take-home policies can all be managed from the same central dashboard.</p> <p>For large school trusts or partners managing filtering for multiple schools, Securly's Multi-School Dashboard provides a dropdown that lets the admin switch across different schools without having to log in separately each time.</p> <p>All activity is also logged in the Audit log for that specific school and can be viewed by the school admin in the Multi-School view.</p>
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		<p>Securly Filter can be applied to managed browsers, and managed devices, with user-level logging and filtering through sign-in with Microsoft Azure/EntraID or Google G-Suite.</p> <p>Securly integrates with Microsoft Azure AD/Entra ID, Windows Server Active Directory, and Google G- Suite to provide user identification.</p> <p>Activity reports contain detailed information about the activity selected for specific users or OUs, including:</p> <ol style="list-style-type: none"> 1. The student and OU/Group names 2. Type of activities that are listed in the report. This depends on what type of activities you select when downloading the report. 3. Policies for which the report is generated. 4. Categories for the activities that are listed. 5. Whether activity has been Allowed, Blocked or Flagged. 6. The date and time stamp of each of the events is listed in each of the rows.

<ul style="list-style-type: none"> Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps 		<p>Securly Aware connects directly to Microsoft Office365 and G-Suite Workspace to scan documents, emails, chats, images, and videos for inappropriate content regardless of where those systems are used or how they are accessed.</p> <p>Securly Filter is a best of breed web filter, however, as some apps communicate using non-HTTP/HTTPS protocols or prevent interception of traffic using end-to-end encryption, this may cause applications to bypass filtering, break or experience unexpected behaviour.</p> <p>We strongly recommend Securly Filter be combined with mobile device management such as Securly MDM to ensure only appropriate applications can be installed.</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		<p>Securly implements multiple language support for both filtering and management interface in English, French, and Spanish.</p> <p>Language support is being continually developed and additional languages will be added as available.</p>
<ul style="list-style-type: none"> Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure) 		<p>As Securly is cloud based it can be implemented at the 'network level' using DNS or network settings and does not require software deployed on devices.</p>
<ul style="list-style-type: none"> Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school 		<p>Securly Filter can be applied to school owned devices regardless of how they access the internet or whether they are within the school network.</p> <p>Securly Filter can also be applied to BYOD schemes, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.</p>

<ul style="list-style-type: none"> • Reporting mechanism – the ability to report inappropriate content for access or blocking 		<p>The Securly block page can be configured to allow staff or students to request sites from the admin.</p> <p>Customers can also make manual submissions via our website.</p> <p>End users also can be provided with a link to submit feedback to administrators.</p>
<ul style="list-style-type: none"> • Reports – the system offers clear historical information on the websites users have accessed or attempted to access 		<p>Securly has designed reports and alerts to be delegated to school management and safeguarding teams to allow quicker response to incidents.</p> <p>Reports are designed with schools in mind and make visually clear which sites are accessed or blocked. Additionally, searches, videos, and social media content are also highlighted.</p> <p>Filters can be applied by user, date/time, category and policy.</p>
<ul style="list-style-type: none"> • Safe Search – the ability to enforce ‘safe search’ when using search engines 		<p>Safe Search can be applied on a policy group basis.</p>

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to *“consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum”*.¹

Please note below opportunities to support schools (and other settings) in this regard

Securly's filtering policies are customisable and policy changes can be applied to specific user groups by the administrator, so that over blocking doesn't occur for certain student groups if they are researching legitimate areas to do with sexual health for due to the requirements of the RHSE and PSHE curriculum.

Securly's primary aim is to enable schools and Multi Academy Trusts to make web experiences safer for students every day. To this end, Securly is committed to partnering with their schools to support and enhance the online experience and deliver a healthy and safe digital environment for all students.

Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsibility digital citizenship. Think Twice, prompts students to reconsider before they send hurtful messages.

Wellness Widget Intervention. When a student's Wellness Level drops, the Wellness Pathways widget will automatically present helpful resources to them on their screen.

Securly are a Student Safety company and are concerned with wellbeing of students beyond web filtering;


- [Securly Aware](#) - Student safety and wellness solution that provides unprecedented visibility into your students' mental health and wellness. Google Drive files, One Drive files, emails, social media, and web searches are scanned to identify indications of suicide, depression, violence, bullying, and nudity.
- [On-call](#) - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now
- [Securly Home](#) - Parent app, a free feature included with your school's Filter purchase, giving parents control over their child's school device when it goes home, including web filtering, site restrictions, and monitored screen time.
- [Classroom](#) - Classroom management tool that works seamlessly across Chrome, Windows, and Mac.
- [MDM](#) - Cloud-based Apple device management for schools.

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree

to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Jarrett Volzer
Position	VP of Product
Date	03/08/2023
Signature	

Appropriate Monitoring for Schools

May 2023



Monitoring Provider Checklist Responses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

Company / Organisation	Securly
Address	Third Floor One London Square, Cross Lanes, Guildford, Surrey, United Kingdom, GU1 1UN https://www.securly.com/
Contact details	uksales@securly.com 0141 343 8322
Monitoring System	Securly Filter, Aware and On-call
Date of assessment	3rd August 2023

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
<ul style="list-style-type: none"> Are IWF members 		Securly has been an IWF member since 01/03/2016
<ul style="list-style-type: none"> Utilisation of IWF URL list for the attempted access of known child abuse images 		<p>Securly receives and incorporates the IWF and CTIRU feeds into its filtering technology</p> <p>Securly blocks access to illegal content including CSAM.</p>
<ul style="list-style-type: none"> Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' 		Securly integrates and block unlawful terrorist content using the list provided by the UK Home Office and Met Police CTIRU (Counter-Terrorism Internet Referral Unit).
<ul style="list-style-type: none"> Confirm that monitoring for illegal content cannot be disabled by the school 		All illegal content categories are locked at a system level. Schools cannot disable these filters.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		Illegal content such as CTIRU list of terrorist content and IWF list of child abuse content are both built into Securly Filter for blocking and monitoring.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		<p>Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsibility and digital citizenship. Think Twice prompts students to reconsider before they send hurtful messages by automatically detecting bullying in typed text and presenting the student with a message immediately.</p> <p>Securly uses AI-powered heuristic tools to provide built-in sentiment analysis which detects bullying content, emails, web searches and social media posts.</p> <p>Securly will flag bullying activity in real-time to enable intervention.</p>
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Securly is an IWF member and fully CIPA compliant. Access to known child abuse and exploitation sites is prevented.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Securly provides a "Hate" category which allows administrators to block access and alert on websites and content which promote hatred and discrimination across race, religion, age, or sex.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Securly provides a "Drugs" category which allows administrators to block access and alert on websites and content which include details of manufacture, sale, and distribution.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Securly includes the CTIRU illegal terrorist content blocklist and provides a "Hate" category. This allows administrators to block access and alert on websites and content which includes promote terrorist organisations and actions, violence and intolerance.
Gambling	Enables gambling		Securly provides a "Gambling" category which allows administrators to block access and alert on websites and content that promotes betting or risky actions for a reward.
Pornography	displays sexual acts or explicit images		Securly provides a "Pornography" category which allows administrators to block access and alert on websites that contain pornographic or explicit images and media.
Self Harm	promotes or displays deliberate self harm		<p>Securly Aware uses AI sentiment analysis to detect self-harm content, emails, web searches and social media posts.</p> <p>Alerts are categorised under the terms 'Self-harm' and 'Grief'</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>

Suicide	Suggest the user is considering suicide		<p>Securly uses AI sentiment analysis which detects content that suggests suicidal ideation in emails, web searches, online docs, and social media posts.</p> <p>Alerts are categorised under the terms 'Self-harm' and 'Grief'</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>
Violence	Displays or promotes the use of physical force intended to hurt or kill		<p>Securly uses AI sentiment analysis which detects violent language towards others in emails, web searches, online docs, and social media posts.</p> <p>Alerts are categorised under the terms 'Violence'</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Securly Filter categories include keywords/phrases, URLs and domains of over the top one million websites.

- Securly PageScan provides automated categorisation of previously unknown websites by scanning the page content and images.
- Selective HTTPS man-in-the-middle decryption to provide real-time, URL filtering, keyword filtering and sentiment analysis.
- Our customers can provide their own block and allow lists in policies and can submit any websites for inclusion in our categories.

Unlike traditional on-premise filtering solutions Securly will selectively intercept to block and filter content. This prevents over blocking or problems with safe content and education services online.

Previously unknown or uncategorised websites will be analysed by Securly Pagescan to accurately determine their content and determine if they need to be filtered.

Administrators also have ability to manage their own safe sites and override Securly categorised websites.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> • Age appropriate – includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access 		Securly can be configured to use GSuite OUs or Azure/EntraID Groups to define separate filtering policies appropriate to different ages or roles. (E.g. Staff, Primary Students, Senior Students).
<ul style="list-style-type: none"> • Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided 		Alerts can be configured at a global level, as well as on a per-policy level. Staff groups can be configured to receive instant alerts about specific groups of students. Administrators can configure scheduled reports to selected users.

<ul style="list-style-type: none"> • Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes. 		<p>Securly administrators can permit or deny by using their own domain names and keywords globally or per policy. Any changes to the system are logged in an audit trail.</p> <p>Reports that are exported from the system are logged separately within the system.</p>
<ul style="list-style-type: none"> • BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location 		<p>BYOD devices on school premises can be monitored using Guest Network policies.</p> <p>BYOD are sometimes enrolled in management systems and could have filtering applied to them whilst off-site although this is not typical.</p>
<ul style="list-style-type: none"> • Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision 		<p>All log data is stored securely within Securly's cloud infrastructure.</p> <p>Measures are taken to ensure compliance with local laws and regulations such as GDPR and DPA. EU customer data resides solely within the EU.</p> <p>Data retention is not currently limited but can be removed at a customer's request.</p>
<ul style="list-style-type: none"> • Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers 		<p>Securly is network based solution and no client-side software is required. Securly is device and operating system agnostic.</p>
<ul style="list-style-type: none"> • Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy 		<p>Administrators can edit policies to include their own custom keywords to allow, block or alert on.</p>

<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>As a cloud-based service, the Securly Safety Console is available anywhere with Internet access.</p> <p>Delegated control can be provided to additional administrators or Safeguarding teams.</p> <p>Multiple sites and take-home policies can all be managed from the same central dashboard.</p> <p>For large school trusts or partners managing filtering for multiple schools, Securly's Multi-School Dashboard provides a dropdown that lets the admin switch across different schools without having to log in separately each time.</p>
<ul style="list-style-type: none"> Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools? 		<p>We recommend schools allow for monitoring within their own Acceptable Usage Policy and IT policies so all users are aware.</p> <p>Securly can assist by providing templates and training webinars on what should be included.</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages? 		<p>Securly implements multiple language support for both filtering and management interface in English, French, and Spanish.</p> <p>Language support is being continually developed and additional languages will be added as available.</p>
<ul style="list-style-type: none"> Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process? 		<p>Securly flag high priority issues in their “flagged” reporting section and alerts are triggered immediately.</p> <p>Additionally, the Securly On-call team can provide additional human review of alerts around the clock and notify emergency contacts or authorities in highest risk cases.</p>

<ul style="list-style-type: none"> Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users. 		<p>Securly Filter can be applied to school owned devices regardless of how they access the internet or whether they are within the school network.</p> <p>Securly Filter can also be applied to BYOD schemes, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.</p>
<ul style="list-style-type: none"> Reporting – how alerts are recorded within the system? 		<p>As well as email all alert events are also recorded to the web dashboard reports or flagged activity section.</p>
<ul style="list-style-type: none"> Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash) 		<p>Securly Aware automatically recall emails containing violence, bullying, or nudity and quarantine images for review by a designated safeguarding lead.</p>

Pro Active Monitoring - how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

Securly offers institutions a range of preventative tools to support student safeguarding and wellness.

Securly Aware creates a Student Wellness Level for every user. SLT or DSLs can quickly identify the students who are trending negatively, drill down into individual student's wellness levels and gain insight into contributing online activities (with Filter). Proactively investigate students who are trending negatively, and provide preventative support and intervention before they become extreme risks

Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsible digital citizenship. Think Twice, prompts students to reconsider before they send hurtful messages.

Wellness Widget Intervention. When a student's Wellness Level drops, the Wellness Pathways widget will automatically present helpful resources to them on their screen.

Recall emails and quarantine images. Securly Aware automatically recalls emails containing violence, bullying, or nudity.

Securly are a Student Safety company and are concerned with the wellbeing of students beyond web filtering;

- [Securly Aware](#) - Student safety and wellness solution that provides unprecedented visibility into your students' mental health and wellness. Google Drive files, One Drive files, emails, social media, and web searches are scanned to identify indications of suicide, depression, violence, bullying, and nudity.
- [On-call](#) - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now
- [Securly Home](#) - Parent app, a free feature included with your school's Filter purchase, giving parents control over their child's school device when it goes home, including web filtering, site restrictions, and monitored screen time.
- [Classroom](#) - Classroom management tool that works seamlessly across Chrome, Windows, and Mac.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

Securly is a student safety company and provides services beyond web filtering and student wellness monitoring.

- On-Call - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now
- Training sessions and material provided to Schools to help follow best practice and integrate Securly technology into their safeguarding procedures.

Securly Filtering and Monitoring Annual Review

- Strategic reviews of filtering and monitoring policies
- Review of adequate filtering and monitoring procedures
- Data assessment and insights: activity, alerts and safeguarding trends

Securly implements multiple language support for both filtering and management interface in English, French, and Spanish.

Securly administrators can permit or deny by using their own domain names and keywords globally or per policy.

Staff members assigned to Faculty Groups can now edit policies that affect OUs or Security Groups assigned to them. This feature can be enabled and disabled at an admin level.

Any changes to the system are logged in an audit trail.

Securly's filtering policies are customisable and policy changes can be applied to specific user groups by the administrator, so that overlocking doesn't occur for certain student groups if they are researching legitimate areas to do with sexual health for due to the requirements of the RHSE and PSHE curriculum.

MONITORING PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Jarrett Volzer
Position	VP of Product
Date	03/08/2023
Signature	