The Beacon

# Safeguarding Children and Young Persons Policy including Online Safety

Based on Keeping Children Safe in Education DfE Guidance September 2026 / Early Years and Foundation Stage Framework 2026 (EYFS)

# Policy

Draft Copy – Awaiting Governor Approval

## Contents


| |
|---|
| Designated Safeguarding Lead and Deputies |
| Safeguarding Governors |
| What to do if you have a welfare concern - flowchart |
| Staff/Visitor access |
| 1. Introduction and Ethos |
| 2. Definition of Safeguarding |
| 3. Context |
| 4. Supporting Policies |
| 5. Key Responsibilities |
| 6. Disclosure |
| 7. Categories of Neglect and Abuse |
| 8. Key Safeguarding Personnel and Procedures |
| 9. Multi-Agency Working |
| 10. Record Keeping |
| 11. Concerns Involving Staff |
| 12. Complaints |
| 13. Staff induction, Awareness and Training |
| 14. Safe Working Practice |
| 15. Staff Supervision and Support |
| 16. Safer Recruitment |
| 17. Preventative Education (Curriculum) |
| 18. Child abuse (Peer to Peer) |
| 19. Bullying |
| 20. FGM |
| 21. CSE |
| 22. Sexting |
| 23. Prevent and Radicalisation |
| 24. HBV “Honour Based” Violence |
| 25. Online Safety |
| 26. Beacon Equality Statement |
| 27. Appendix One – Indicators of Abuse |
| 28. Update Schedule |


DRAFT

# AWAITING NEW POSTER

| | | | |
|---|---|---|---|
| **Julie Howell**<br>MAST Safeguarding Lead – Lead DSL | | **Casey Fletcher**<br>Head of School / Lead DSL | |
| **Russell Ames**<br>AHT & Behaviour Lead / DDSL | | **Ady Young**<br>Executive Head / DDSL | |
| **Naomi Fuller**<br>MAST Officer / DDSL | | **Bethan Griggs**<br>Pupil Support Manager | |
| **Ellie Garrett**<br>Mental Health Lead/DDSL | | **Kirsten McGill**<br>MAST Officer / DDSL | |
| **Rebecca Loynds**<br>Assistant Head Teacher/DDSL | | **Donna Wickens**<br>Assistant Head Teacher/DDSL | |
| **Hayleigh Graves**<br>Walmer Assistant Head Teacher/ DDSL | | **Caroline Pratt**<br>Assistant Head Teacher/DDSL | |
| **Samantha Barnes**<br>Online Safety DDSL | | **Chris Wallis**<br>Assistant Head Teacher/DDSL | |

**What to do if you have a welfare concern in The Beacon**

Why are you concerned?

- For example
  - Allegation/ child shares a concern or worry
  - Indicators of abuse or neglect

Immediately record your concerns

- Follow the school's procedure
  - Reassure the child
  - Clarify concerns if necessary (**TED**: **T**ell, **E**xplain, **D**escribe)
  - Use child's own words
  - Sign and date your records

Inform the Designated Safeguarding Leads: Casey Fletcher / Julie Howell or any Deputy DSL

Designated Safeguarding Lead

- Consider whether the child is at immediate risk of harm e.g. unsafe to go home
- Access the '2026' KSCMP Support Level Guidance document and procedures:
- Refer to other agencies as appropriate e.g. internal or community services, LESAS,

If you are unhappy with the response

Staff:

- Follow local escalation procedures
- Follow Whistleblowing procedures

Pupils and Parents:

- Follow school complaints procedures as published on our website

Record decision making and action taken in the pupil's Child Protection/Safeguarding file within 24 hours

Monitor
Be clear about:

- What you are monitoring e.g. behaviour trends, appearance etc.

Review and request further support (if necessary)

DRAFT

At all stages the child's circumstances will be kept under review
The DSL/Staff will request further support if required to ensure the **child's safety** is **paramount**

**The Beacon Access**

**Identifying individuals that access the site.**

Adults who need to access the school can be identified by the following lanyards, some of which are equipped with electronic keys enabling them to access certain areas of the school:

| | |
|---|---|
| The Beacon - staff | Staff directly employed by The Beacon<br>Access all learning areas |
| The Beacon – visitor | Visitors - Including maintenance/people on courses/people accessing the café<br>Escorted by The Beacon or MASH staff |
| The Beacon - MHFA | Mental Health First Aiders |
| Beacon Plus - staff | Beacon Plus staff |
| Governors | The school governors can access the non-pupil areas of the school. Governors have access to all learning areas accompanied by relevant staff. |
| Pupil/Student Leaders | Student leaders are usually accompanied by a staff member |
| NHS/Health | These adults are employed by the NHS/Health and hold an NHS – DBS these details are confirmed by the NHS. They can access most areas in line with their roles (designated MASH areas) |

There is a leaflet in reception with basic Safeguarding information and the names of the Designated Safeguarding Leads

DRAFT

## 1. Introduction and Ethos: Safeguarding Children and Young Persons Policy

This is a core policy that forms part of the induction for all staff. It is a requirement that all members of staff have access to this policy and sign to say they have read and understood its contents.

This policy will be reviewed at least annually and/or following any updates to national and local guidance procedures

**Safeguarding Children and Young Persons Policy Document**

Safeguarding and promoting the welfare of children refers to the process of protecting children from abuse or neglect, preventing the impairment of their health or development, ensuring that children grow up in circumstances consistent with the provision of safe and effective and nurturing care and undertaking that role so as to enable those children to have optimum life chances and to enter adulthood successfully.

**The Beacon, through the embedding of its Core Values, will ensure that all children and young people have the same protection regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity. The Beacon is committed to anti-discriminatory practice and will recognise the additional needs of children from minority ethnic groups and disabled children and the barriers they may face, especially around communication.**

Staff and Governors alike have a duty to ensure that our pupils are safe not only when attending The Beacon but also in the wider community.

Ensuring that the Safeguarding Policy is updated as and when required is the responsibility of the Designated Safeguarding Lead. The identifiable individual is the Safeguarding Lead. In his/her absence it becomes the responsibility of the Headteacher and the Safeguarding Governor.

The Beacon is a community and all those directly connected (staff, volunteers, governors, parents, families and pupils) have an essential role to play in making it safe and secure. The Beacon recognises its statutory responsibility to safeguard and promote the welfare of all children.

The Beacon recognises the importance of providing an ethos and environment within school that will help children to be safe and feel safe. In our school children are respected and encouraged to talk openly.

Our school core safeguarding principles are:

- We are an important part of the wider safeguarding system for children.
- It is our whole school's responsibility to safeguard and promote the welfare of children.
- All children (defined as those up to the age of 18) and young adults regardless of age, gender, ability, culture, race, language, religion or sexual identity, have equal rights to protection.
- All children have a right to be heard and to have their wishes and feelings taken into account.

DRAFT

- All our staff understand safe professional practice and adhere to our safeguarding policies.

**Aim**

We believe that procedures and processes in place at The Beacon are robust and embedded, keeping our pupils and staff safe.

**School policy, ethos and training**

We promote healthy friendships and relationships through our whole school ethos.

Our induction package ensures that staff at The Beacon are aware of indicators and how to report concerns and how to contact other agencies if required, supported by the Multi Agency Support Team.

The Beacon also displays posters and distributes leaflets to advertise services that children can use to get information and advice about sexual exploitation, which is covered in annual staff training and through P.S.H.E.

## 2. Definition of Safeguarding

*"Safeguarding is not just about protecting children from deliberate harm. It includes a wide range of issues relating to pupil's welfare, health and safety." (Inspecting safeguarding in early years, education and skills, Ofsted - new framework/toolkit 2025.)*

All safeguarding policies will be reviewed on an annual (minimum) basis by the Governing Body which has responsibility for oversight of school safeguarding and child protection systems. The Designated Safeguarding Lead/Head of School will ensure regular reporting on safeguarding activity and systems in school to the Governing Body. The Governing Body will not receive details of individual pupil situations or identifying features of families as part of their oversight responsibility.

There are four main elements to our Child Protection Policy

- **Prevention** (e.g. positive, supportive, safe school culture, curriculum and pastoral opportunities for children, safer recruitment procedures);
- **Protection** (by following the agreed procedures, ensuring all staff are trained and supported to respond appropriately and sensitively to safeguarding concerns);
- **Support** (for all pupils, parents and staff, and where appropriate specific intervention for those who may be at risk of harm);
- **Working with parents and other agencies** (to ensure appropriate communications and actions are undertaken).

The procedures contained in this policy apply to all staff (including temporary staff and volunteers) and governors and are consistent with those of Kent Safeguarding Children Multi-Agency Partnership (KSCMP).

DRAFT

## 3. Context

This policy has been developed in accordance with the principles established by the Children Acts 1989 and 2004 and related guidance. This includes:
DfE guidance Keeping Children Safe in Education 2026(KCSIE)
Working Together to Safeguard Children 2026 (WTSC)
Ofsted guidance 'Inspecting safeguarding in early years, education and skills' (2016)
Framework for the Assessment of Children in Need and their Families (2000)
Kent and Medway Safeguarding Children Procedures (Online)
Early Years and Foundation Stage Framework 2026 (EYFS)

*Section 175 of the Education Act 2002 requires school governing bodies, local education authorities and further education institutions to make arrangements to safeguard and promote the welfare of all children who are pupils at a school, or who are students under 18 years of age. Such arrangements will have to have regard to any guidance issued by the Secretary of State.*

The school acknowledges that this policy recognises a range of specific safeguarding issues including (but not limited to):

- Bullying (including cyberbullying)
- Upskirting
- Children Missing Education (CME)
- Child missing from home or care
- Child Sexual Exploitation (CSE)
- Domestic violence
- Drugs and alcohol misuse
- Fabricated or induced illness
- Faith abuse
- Female Genital Mutilation (FGM)
- Forced marriage
- Gangs and youth violence
- Gender based abuse and violence against women and girls
- Hate
- Honour based abuse
- Mental health
- Missing children and adults
- Online safety
- Prevent duty (radicalisation and extremism)
- Private fostering
- Relationship abuse
- Sharing nudes and semi-nudes (previously sexting)
- Human trafficking and modern slavery

## 4. Supporting Policies

Attendance Policy
Managing Allegations against Staff Policy

Links to Other Agencies

KSCMP - Kent Safeguarding Children's' Multi-Agency Partnership
http://www.kscmp.org.uk/

DRAFT

NSPCC - National Society for the Prevention Cruelty to Children
https://www.nspcc.org.uk/

Meeting digital and technology standards in schools and colleges
Meeting digital and technology standards in schools and colleges - Cyber security: core standard - Guidance

**Terminology**

**Child protection** refers to the processes undertaken to meet statutory obligations laid out in the Children Act 1989 and associated guidance (see Keeping Children Safe in Education Working Together to Safeguard Children, An Interagency Guide to Safeguard and Promote the Welfare of Children) in respect of those children who have been identified as suffering, or being at risk of suffering harm.
**Staff** refers to all those working for or on behalf of the school, full time or part time, in either a paid or voluntary capacity.

**Child/pupil** refers to all young people including those who are in 6th form and or are 19 years old.

**Parent/Carers** refers to birth parents and other adults who are in a parenting role, for example step-parents, foster carers and adoptive parents.

## 5. Key Responsibilities

**Designated Safeguarding Leads (DSL)**

The school has appointed 2 members of the leadership team, Casey Fletcher and Julie Howell, as the Designated Safeguarding Leads (DSL). The DSL's have overall responsibility for the day to day oversight of safeguarding and child protection systems in school.

The DSL will undergo appropriate and specific training to provide them with the knowledge and skills required to carry out their role. The DSL and any deputy DSLs training will be updated formally every two years but their knowledge and skills will be updated through a variety of methods at regular intervals and at least annually.

Deputy DSLs are trained to the same standard as the DSL. Whilst the activities of the DSL may be delegated to the deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL and this responsibility will not be delegated.

**It is the role of the DSL to:**

Act as the central contact point for all staff to discuss any safeguarding concerns
Maintain a confidential recording system for safeguarding and child protection concerns

- Coordinate safeguarding action for individual children

DRAFT

- In the case of Children Looked After the DSL should have the details of the child's social worker and the name of the virtual school head in the authority that looks after the child ( DSL liaising closely with the CiC officer)
- Liaise with other agencies and professionals in line with Working Together to Safeguard Children 2026
- Ensure that locally established referral procedures are followed as necessary
- Represent, or ensure the school is appropriately represented at multi-agency safeguarding meetings (including Child Protection conferences)
- Manage and monitor the school's role in any multi-agency plan for a child.
- Be available during term time (during school hours) for staff in the school to discuss any safeguarding concerns
- Ensure all staff access appropriate safeguarding training and relevant updates in line with the recommendations within Keeping Children Safe in Education 2026

**Members of Staff**

**All members of staff have a responsibility to:**

Provide a safe environment in which children can learn.
Be prepared to identify children who may benefit from early help.
Understand the early help process and their role in it.
Understand your schools safeguarding policies and systems.
Undertake regular and appropriate training which is regularly updated.
Be aware of the process of making referrals to children's social care and statutory assessment under the Children Act 1989.
Know what to do if a child tells them that he or she is being abused or neglected.
Know how to maintain an appropriate level of confidentiality.
Be aware of the indicators of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection.
Be aware of their responsibilities outside of school hours.

**Children and Young People**

**Children and young people (pupils) have a right to:**

Contribute to the development of school safeguarding policies.
Receive help from a trusted adult.
Learn how to keep themselves safe, including online.

**Parents and Carers**

**Parents/carers have a responsibility to:**

Understand and adhere to the relevant school/policies and procedures.
Talk to their children about safeguarding issues with their children and support the school in their safeguarding approaches.
Identify behaviours which could indicate that their child is at risk of harm including online and seeking help and support from the school, or other agencies.

Parents can obtain a copy of the school Child Protection Policy and other related policies on request and can view them via the school website (http://learn.thebeacon.kent.sch.uk/document-archive/).

DRAFT

## 6. Disclosure

A child/young person may tell you that he/she has been abused. Alternatively, you may have good reason to suspect that abuse is taking place. Where the child/young person feels able to talk about abuse to an adult, it is generally a sign of a strong and trusting relationship. Any conversation with a child/young person should be held in a quiet area where there are not likely to be any interruptions but ***do*** let a colleague know for your own protection. You should be aware of the importance of adopting a supportive role and the child/young person must not be subjected to lengthy or multiple discussions as this could confuse the child/young person and jeopardise the evidence. Please refer to school procedures for record keeping at the end of the document.

The Beacon celebrates a robust culture of keeping everyone safe, educated and well informed. Training for staff, pupils, parents/carers and governance is enhanced by written documentation and embedded safeguarding processes.
This includes:

An environment that acknowledges and supports challenge
An environment where everyone is treated as an individual
An environment that provides all the relevant resources required to keep people safe

The Beacon will always have a Designated Safeguarding Lead or Deputy on site during usual school hours. The Designated Safeguarding Team is displayed in key areas in the school including public areas and all classrooms. At the Walmer site posters are displayed in classrooms and on the information board in Reception areas.

Sensitive information, in line with General Data Protection Regulations (GDPR), is securely locked within locked filing cabinets in a room locked with a numeric keypad to which only relevant staff have access. At the Walmer site, there are no filing cabinets onsite. Any sensitive information remains onsite at Folkestone or on CPOMS.

Designated Safeguarding Leads
MAST officers
Senior Leadership Team
Site Team (Cleaners) only where necessary

Only information that is relevant in keeping each individual safe is shared between agencies. A record of what has been shared is kept by the Multi Agency Support Team.

## 7. Categories of Neglect and Abuse

(Key indicators of abuse included in appendix one, page 47)

- **Physical Abuse -** Causing physical harm to a child – slapping, kicking, rough handling, twisting of limbs, misuse of medicines, inappropriate sanction or restraint.
- **Neglect (Acts of omission) -** persistent failure to meet a child's needs – physical and/or psychological, ignoring medical and/or physical care needs (inhalers), non-referral to appropriate agencies, inadequate necessities in life such as nutrition/heating, clothing.
- **Sexual Abuse -** Involving a child in sexual activity – rape, sexual assault where the individual for whatever reason was not able or legally able to give consent, involvement in pornography against the individual's will (internet/mobile phones).

DRAFT

- **Emotional Abuse/Psychological Abuse -** Persistent emotional ill treatment of a child – verbal assault or intimidation, deprivation of contact, threats of harm and or abandonment. Humiliation, being made to feel unloved, abuse of ability to make choices.

Although the indicators above are the four main categories, abuse can also be defined in the following areas:

- **Financial Abuse –** theft of an individual's money, exploitation, pressure to make and inappropriate will.
- **Discriminatory Abuse –** usually aimed at oppression and attitudes towards gender, religion, sexual orientation, physical/sensory impairment and age.
- **Institutional Neglect and Poor Practice –** this may take the form of isolated incidents of poor or unsatisfactory practice (not completing paperwork in a timely manner) at one end of the spectrum, through to persuasive ill treatment or gross misconduct (not reporting a discloser through the appropriate channels).
- **Self-Neglect –** has been recognised within the care act 2014 as part of the safeguarding framework.

**Indications of abuse in young people who have disabilities/medical needs**

The Beacon acknowledges that children with special educational needs (SEN) and disabilities can face additional safeguarding challenges as they may have an impaired capacity to resist or avoid abuse.

The Beacon will ensure that children with SEN and disabilities, especially those with communication difficulties, will be supported to ensure that their voice is heard and acted upon.

Members of staff are encouraged to be aware that children with SEN and disabilities can be disproportionally impacted by safeguarding concerns such as bullying. All members of staff will be encouraged to appropriately explore possible indicators of abuse such as behaviour/mood change or injuries and not to assume that they are related to the child's disability and be aware that children with SEN and disabilities may not always outwardly display indicators of abuse.

It is better to report a hundred cases where no abuse is occurring than to miss one case. Any worry or concern about a child must be reported.

**Attendance and Children Missing Education**

The Beacon recognises that children who are absent from Education, as well as Children Missing Education, may be at increased risk of abuse, neglect, child sexual exploitation, child criminal exploitation and other safeguarding risks.
Attendance concerns will be considered within safeguarding decision making and early intervention processes.

## 8. Key Safeguarding Personnel and Procedures

The Beacon will ensure that there are trained Designated Safeguarding Leads (DSLs) available during the hours of 8am and 4:30pm pm Monday to Friday (covering the school day/breakfast/after school clubs). Any urgent safeguarding concerns out of these times should be directed to the out-of-hours duty team on 03000 411111 or if someone is in immediate danger then call 999 for emergency services.

DRAFT

School based DSLs will:

- Keep online and, where necessary, records of any concerns/investigations.
- Refer concerns/investigations to appropriate agencies (Social Services/Early Help/Police). Attend/contribute to Child Protection Conferences.
- Provide face-to-face Safeguarding Training to staff as part of their induction.
- Coordinate The Beacons' policy on Child Protection procedures.
- Develop effective links to appropriate agencies.
- Be instrumental in updating Safeguarding Policy.
- Liaise with the nominated Safeguarding Governor.
- Inform staff of changes as soon as practically possible.
- Attend additional training as required.
- Ensure that all relevant local and national changes or updates to safeguarding policy and procedures are communicated to all staff.

If a child/young person chooses to talk to you and discloses that he/she has been abused:

| | | |
|---|---|---|
| A | Confidentiality | Never tell the child/young person and or adult you will keep secret what they have told you. Tell the child/young person you must talk to other people who can help. Ask with whom he/she wants to talk? |
| B | Listen | Repeat the child's/young person's words - to ensure you are hearing them correctly. |
| C | Stop | Do not be tempted to ask more questions than necessary - this could confuse the child/young person. |
| D | Reassure | Explain to the child/young person they are not to blame. |
| E | Believe | Explain to the child/young person you believe what they are telling you. |
| F | Affirm | I am glad you told me? It was right to tell. You have been brave to tell me etc. |
| G | Follow up | Make arrangements with the child/young person to speak to them later. They have chosen you as the adult they can trust. |
| H | Report | Immediately report what you have heard to a Designated Safeguarding Lead Report verbally and write, verbatim, what the child/young person has said to you.<br>Remember to date and sign what you have written. Use a body map if necessary. |
| I | Examination | Do not attempt an examination or remove a child's/young person's clothes to look further at an injury. The child/young person should only be examined by an appropriate doctor. It may be possible to observe the child/young person during the normal school routine - physical education or swimming. If a child/young person wants to show you his/her injuries, make sure that a colleague is with you as a witness. Try to arrange for one of you to be of the same sex as the child/young person. |

The following factors may contribute to a child/young person's difficulty in explaining what has happened:

- They cannot find the words to say what is happening because of age, learning, language and hearing difficulties.
- They do not have an adult's permission to tell, and actual or implied threats have been used.
- They have found they cannot trust a parent or an adult who they believed they knew well.
- They assume that they will not be believed.

DRAFT

- They believe silence will help to protect others in their family.
- They have been forced to take the blame for what is happening.
- They do not know what the alternatives are or have access to agencies which can offer protection and/or help.

DRAFT

- They are not yet ready to talk about their experience - they do not feel safe enough.

Child/Young Person Protection - guidance on procedures for responding to allegations or suspicions of abuse.

- The school (through a DSL) **is required to make a referral within 24 hours** (in writing or with written confirmation of telephoned referral) of disclosures of allegations or suspicions of abuse, or other actual or likely significant harm to a child/young person, to the local social services department rather than investigation by the school.

- There is a requirement for joint consideration between the school and the local social services department of subsequent actions, including continuing protection of children and adults in the light of the allegation or suspicion, and when and how to inform any person who is the subject of the allegation or suspicion, and the parents/carers of each child involved.

- The placing authorities of the child/young person involved must be notified of any allegation or suspicion of abuse and of the initiation and outcome of any child/young person protection enquiries (under Section 47 of the Children Act 1989) involving the school.

- Any evidence known of children/young people becoming involved in prostitution or of unauthorised people picking children/young people up, contacting children/young people in the school, or observed trying to make contact with the children/young people outside of the school must be reported by a DSL.

- The school should consider measures that may be necessary to protect individual children/young people following an allegation or suspicion of abuse being made.

- If a member of staff feels that practices in the school could put pupils at risk of serious harm or abuse, they must first raise their concerns with a DSL. If a member of staff is concerned with the way in which the school manages the issue, they can contact Governors and/or Ofsted.

## 9. Multi-agency Working

The Beacon recognises and is committed to its responsibility to work with other professionals and agencies in line with statutory guidance (WTSC 2026)

Schools are not the investigating agencies when there are concerns about child protection. We will, however, contribute to the investigation and assessment processes as required. The Beacon recognises the importance of multi-agency working and will support attendance at relevant safeguarding meetings, including Child Protection Conferences, Core Groups, Strategy Meetings, Child in Need meetings or other Family Help multi-agency meetings.

- The School Leadership Team and DSL will work to establish strong and co-operative relationships with relevant professionals in other agencies.

**Confidentiality and Information Sharing**

- The Beacon recognises that all matters relating to child protection are confidential. The Headteacher or DSL will only disclose information about a pupil to other members of staff on a 'need to know' basis.

DRAFT

- All members of staff must be aware that whilst they have duties to keep any information confidential, they also have a professional responsibility to share information with other agencies to safeguard children.

- All staff must be aware that they cannot promise a child to keep secrets which might compromise the child's safety or wellbeing.

- DfE Guidance on Information Sharing (September 2026) provides further detail.

## 10. Record Keeping – Child/Adult Protection

Staff will record any welfare concern that they have about a child on the school's safeguarding system CPOMS (with a body map if injuries have been observed) and send them without delay to MAST. Records will be completed as soon as possible after the incident/event, using the child's words and will be recorded on the online CPOMS platform.

All safeguarding concerns, discussions and decisions (and justifications for those decisions) will be recorded on the original document where possible. If members of staff are in any doubt about recording requirements, they should discuss their concerns with DSL.

Safeguarding concerns are registered on the CPOMS Safeguarding section online

- Safeguarding records are kept for individual children and are maintained separately from all other records relating to the child in the school. Safeguarding records are kept in accordance with data protection legislation and are retained centrally and securely by the DSL. Safeguarding records are shared with staff on a 'need to know' basis only.

- All safeguarding records will be transferred in accordance with data protection legislation to the child's subsequent school/setting, under confidential and separate cover. These will be given to the new DSL and a receipt of delivery will be obtained.

- Detailed guidance on record keeping is found in a separate document "Guidelines for Safeguarding Record Keeping in Schools".

- The Headteacher will be kept informed of any significant issues by the DSL.

If small concerns are not recorded and passed to a central source, the DSL, it is possible that an incomplete picture of a particular child/young person may be held by a number of staff members who, if they collated the information, would find that a much more worrying picture was emerging. The DSL should be in a position to build up the jigsaw and can only do so if all staff members record and share all their concerns.

If detailed records are maintained, it is possible for the school to respond quickly and efficiently to requests for information from other agencies, especially from Social Services, who will ask the school for information on any child/young person of school age who has been referred to them from any source.

**Walmer Safeguarding Folders**

Safeguarding folders for all Walmer pupils/students remain on site at Folkestone. This ensures updates can be recorded in a timely manner and can be accessed by MAST Safeguarding Team throughout the day.

DRAFT

The records serve as a database for future decisions.

Walmer is currently supported on site by an AHT DDSL and Executive Head DDSL, MAST SG Team cover three days per week.

## 11. Concerns involving members of staff

- The Beacon recognises that it is possible for staff and volunteers to behave in a way that might cause harm to children and take seriously any allegation received. Such allegations should be referred immediately to the Executive Head or Head of School in their absence who will first contact the Local Authority Designated Officer (LADO) to agree further action to be taken in respect of the child and staff member. In the event of allegations of abuse being made against the Executive Head or Head of School then staff are advised that allegations should be reported to the Chair of Governors who will contact the LADO in the first instance.

- All staff and volunteers should feel able to raise concerns about poor or unsafe practice and such concerns will always be taken seriously by the senior leadership team.

- All members of staff are made aware of the school's whistleblowing procedure and that it is a disciplinary offence not to report concerns about the conduct of a colleague that could place a child at risk. Staff can also access the NSPCC whistleblowing helpline if they do not feel able to raise concerns regarding child protection failures internally. Staff can call: 0800 028 0285 (8:00 AM to 8:00 PM Monday to Friday) or email: help@nspcc.org.uk

- The Beacon has a legal duty to refer to the Disclosure and Barring Service (DBS) anyone who has harmed, or poses a risk of harm, to a child, or if there is reason to believe the member of staff has committed one of a number of listed offences, and who has been removed from working (paid or unpaid) in regulated activity, or would have been removed had they not left. The DBS will consider whether to bar the person. If these circumstances arise in relation to a member of staff at our school, a referral will be made as soon as possible after the resignation or removal of the individual in accordance with advice from the LADO and/or Schools Personnel Service.

All staff need to be aware that it is a disciplinary offence NOT to report concerns about the conduct of a colleague that could place a child at risk.

**When in doubt – Consult**

Failure to immediately report any actual or suspected physical, sexual or emotional abuse or neglect of a child/young person is a disciplinary offence.

## 12. Complaints

- The school has a **Complaints Procedure** available to parents, pupils and members of staff and visitors who wish to report concerns. This can be found on our website.

- All reported concerns will be taken seriously and considered within the relevant and appropriate process. Anything that constitutes an allegation against a member of staff or volunteer will be dealt with under the specific **Procedures for Managing**

DRAFT

**Allegations against Staff policy.** This can be found on our website.

## 13. Staff Induction, Awareness and Training for Safeguarding Policy

- All members of staff have been provided with a copy of Part One of "*Keeping Children Safe in Education"* (2026) which covers Safeguarding information for all staff.
  All staff, irrespective of role, will read and understand Part One of Keeping Children Safe in Education 2026.
  The previous Annex A summary has been removed. Staff will confirm in writing that they have read and understood the statutory safeguarding expectations outlined in Part One.
  DSL's, DDSL's and Governors will read the entire document.

- The DSL will ensure that all new staff and volunteers (including temporary staff) are aware of the school's internal safeguarding processes.

- All staff members (including temporary staff) will receive training to ensure they are aware of a range of safeguarding issues.

- All staff members (including temporary staff) will receive regular safeguarding and child protection updates, at least annually.

- All staff members (including temporary staff) will be made aware of the school's expectations regarding safe and professional practice via the staff Behaviour policy (or code of conduct) and ICT Acceptable Use Policy.

- The DSL will provide an annual report to the Governing Body detailing safeguarding training undertaken by all staff and will maintain up to date register of who has been trained.

- Although the school has a nominated lead for the governing body, all members of the governing body will access appropriate safeguarding training which covers their specific strategic responsibilities on a regular basis.

## 14. Safe Working Practice

- All members of staff are required to work within clear guidelines on Safe Working Practice/the school's Code of Conduct.

- Staff should be aware of the school's **Behaviour Management and Physical Intervention Policies***,* and any physical interventions must be in line with agreed policy and procedures.
- Staff should be particularly aware of the professional risks associated with the use of social media and electronic communication (email, mobile 'phones, texting, social network sites, etc.) and should adhere to the school's online safety and acceptable use policies.

## 15. Staff Supervision and Support

- Any member of staff affected by issues arising from concerns for children's welfare or safety can seek support from the DSL.

DRAFT

- The induction process will include familiarisation with child protection responsibilities and procedures to be followed if members of staff have any concerns about a child's safety or welfare.

**The school will provide support for all members of staff through training and conversation to ensure that:**

- All staff are competent to carry out their responsibilities for safeguarding and promoting the welfare of children

- All MAST safeguarding staff can be supported by the DSL in their role.

- All members of staff have reviews of their own practice to ensure they improve over time with training; scenario walk throughs and knowledge testing.

The DSL will also put staff in touch with outside agencies for professional support if they wish. Staff can also approach organisations such as their Union, the Education Support Partnership or other similar organisations directly.

- The school will ensure that members of staff who are working within the foundation stage are provided with appropriate supervision in accordance with the statutory requirements of Early Years Foundation Stage Framework (EYFS) 2026.

## 16. Safer Recruitment

The Beacon is committed to ensure that we develop a safe culture and that all steps are taken to recruit staff and volunteers who are safe to work with our pupils and staff.

- The Governing Body and Leadership Team are responsible for ensuring that the school follows safe recruitment processes outlined within guidance.

The Beacon is responsible for ensuring that the school maintains an accurate Single Central Record (SCR) in line with statutory guidance.

- The Governing Body will ensure that there is at least one of the persons who conducts an interview has completed safer recruitment training.

- We are also committed to supporting the statutory guidance from the Department for Education on the application of the Childcare (Disqualification) Regulations 2009 and related obligations under the Childcare Act 2006 in schools.
- We advise all staff to disclose any reason that may affect their suitability to work with children including convictions, cautions, court orders, cautions, reprimands and warnings.

## 17. Preventative Education/Procedures

The Beacon implements and adopts sound policies and procedures on the management or situations where there is suspected abuse, supported through the curriculum (P.S.H.E.). This helps pupils and students acquire relevant information, skills and attitudes both to resist abuse in their own lives and to prepare them for the responsibilities of their adult lives, including parenthood.
Where appropriate The Beacon will include specific teaching about the risks of child abuse

DRAFT

and how pupils can protect themselves, within their personal and social education programmes.

In addition to the regular safeguarding training which includes types of abuse and their indicators the following is also mandatory for staff/volunteers and offered to parents/carers, multi-agency;

Female Genital Mutilation
Child Sexual Exploitation
Prevent Strategy
Online safety
Sharing nudes and
semi-nudes
Child on Child Abuse

The Beacon delivers safeguarding information/training in many ways as follows;

- Directly to the pupils through P.S.H.E.
- Targeted training to individuals and/or groups as required where a current trend has been identified by the Multi Agency Support Team.
- Training to Staff and Governors.
- Training to parents/carers to cover planned contextual areas agreed in Parent Voice.
- Annual on-line to all staff.
- Staff induction, completed in the first week of employment before staff work with the pupils.
- Regular updates on training days, through zone meetings or when appropriate.

Parents/ad hoc visitors accessing The Beacon are to remain in the main reception/café area, they must be accompanied by a checked adult identifying themselves.
Policies and procedures are always available to staff.
Within The Beacon, the Multi Agency Support Team (MAST) have literature to help staff in the safeguarding of the pupils. Staff can seek guidance from any DSL/DDSL in The Beacon.

## 18. Early Years safeguarding

The Beacon recognises that children in the Early Years Foundation Stage (EYFS) are particularly vulnerable because of their age, developmental stage, communication needs and dependence upon adults for their care and protection.
Safeguarding arrangements within Early Years therefore reflect the requirements of Keeping Children Safe in Education (KCSIE), the EYFS statutory framework, *Working Together to Safeguard Children* and the school's wider safeguarding and child protection procedures.

## 19. Child Abuse by Another Child (Child on Child)

We recognise that children can abuse their peers. Abuse will never be tolerated or passed off as “banter”, “just having a laugh” or “part of growing up”.
All child-on-child abuse is unacceptable and will be taken seriously regardless of the gender involved.
Most cases of pupils hurting other pupils will be dealt with under our school’s normal procedures, but this child protection and safeguarding policy will apply to any allegations

DRAFT

that raise safeguarding concerns. This might include where the alleged behaviour:

- Is serious, and potentially a criminal offence
- Could put pupils in the school at risk
- Is violent
- Involves pupils being forced to use drugs or alcohol
- Involves sexual exploitation, sexual abuse or sexual harassment, such as indecent exposure, sexual assault, upskirting or sexually inappropriate pictures or videos (including sexting)

**If a pupil makes an allegation of abuse against another pupil:**

You must record the allegation and tell the DSL, but do not investigate it.
The DSL will contact the local authority children's social care team and follow its advice, as well as the police if the allegation involves a potential criminal offence.
The DSL will put a risk assessment and support plan into place for all children involved (including the victim(s), the child(ren) against whom the allegation has been made and any others affected) with a named person they can talk to if needed.
The DSL will contact the children and adolescent mental health services (CAMHS), if appropriate.

**We will minimise the risk of peer-on-peer abuse by:**

Challenging any form of derogatory or sexualised language or behaviour, including requesting or sending sexual images. We will be mindful of the need to explain in age/stage/need type appropriate language the meaning and appropriateness of what has been said or done.
Being vigilant to issues that particularly affect different genders – for example, sexualised or aggressive touching or grabbing towards female pupils, and initiation or hazing type violence with respect to boys.
Ensuring our curriculum helps to educate pupils about appropriate behaviour and consent.
Ensuring pupils know they can talk to staff confidentially by approaching their form teacher or any responsible adult at The Beacon.
Ensuring staff are trained to understand that a pupil harming a peer could be a sign that the child is being abused themselves, and that this would fall under the scope of this policy.

Evidence suggests that some abused young people may themselves begin to abuse. All members of staff need to be aware of this and ensure extra vigilance, in those situations where one child/young person may be able to take advantage of another.
When abuse of a child/young person is alleged to have been carried out by another child/young person, it is important that the Safeguarding Children Procedure is followed in respect of both the victim and the alleged abuser. Adolescent abusers are themselves in need of services.

**Violence Against Women and Girls (VAWG)**

The Beacon recognises the importance of preventing Violence Against Women and Girls (VAWG), misogyny, harmful gender stereotypes and harmful sexual behaviour. Staff will challenge inappropriate attitudes and behaviours, promote respectful relationships and respond promptly to concerns regarding sexual harassment, sexual violence and gender-based abuse

DRAFT

## 20. Bullying

Bullying (both emotional and physical can constitute a child protection issue) Please refer to the anti-bullying policy.

## 21. Female Genital Mutilation (FGM)

**If you discover that FGM has taken place or a pupil is at risk of FGM:**

The Department for Education's Keeping Children Safe in Education 2026 explains that FGM comprises "all procedures involving partial or total removal of the external female genitalia, or other injury to the female genital organs".

FGM is illegal in the UK and a form of child abuse with long-lasting, harmful consequences. It is also known as 'female genital cutting', 'circumcision' or 'initiation'.

Unless you have been specifically told not to disclose, you should also discuss the case with the DSL and involve children's social care as appropriate.

Any other member of staff who discovers that an act of FGM appears to have been carried out on a pupil under 18 must speak to the DSL and follow our local safeguarding procedures.

The duty for staff mentioned above does not apply in cases where a pupil is at risk of FGM or FGM is suspected but is not known to have been carried out. Staff should not examine pupils.

Any member of staff who suspects a pupil is at risk of FGM or suspects that FGM has been carried out [if relevant or discovers that a pupil aged 18 or over appears to have been a victim of FGM] must speak to the DSL and follow our local safeguarding procedures.

**Actions**

Any teacher who discovers (either through disclosure by the victim or visual evidence) that an act of FGM appears to have been carried out on a pupil under 18 must immediately report this to the police, personally. This is a statutory duty, and teachers will face disciplinary sanctions for failing to meet it.

Staff across The Beacon receive face-to-face training on FGM as part of their induction package, including how to report record concerns.

**The Daughters of Eve** website helps to raise awareness of this issue and sign-posts those affected by it to supportive services: http://www.dofeve.org/

## 22. Child Sexual Exploitation

We believe that at The Beacon we are well placed to teach pupils how to make positive choices and informed decisions in their relationships so that they can protect themselves

DRAFT

from sexual and criminal exploitation. Positive relationships with school staff will encourage children to disclose any worries about their own safety or the safety of another pupil.

We promote healthy friendships and relationships through our whole school ethos, there are numerous policies in place to ensure staff have the right information and guidance to ensure they are equipped to keep the pupils and themselves safe. There is a commitment from senior management and governors at The Beacon to deal with the issue of child sexual exploitation.

There are at least two Designated Safeguarding Leads on site at any one time, supported by a Safeguarding and Health and Safety Governor.

Staff are taught the indicators to look out for in regard to Child Sexual Exploitation: safeguarding underpins their Core Values. Staff advocate appropriately for the pupils and their families.

## 23. Sharing nudes and semi-nudes (including Youth Produced Sexual Imagery)

Even if explicit material is sent or elicited without malicious intent the consequences are serious and put those involved at risk of serious harm. Having or sending explicit material on digital devices is also a criminal offence for those under 18. Pupils are taught about sharing nudes and semi-nudes as part of their e-safety and online safety education. The school takes incidences of sharing nudes and semi-nudes extremely seriously, and deals with them in accordance with child protection and safeguarding procedures, including reporting to the police.

**Your responsibilities when responding to an incident:**

If you are made aware of an incident involving (also known as youth produced sexual imagery) you must report it to a DSL / DDSL immediately.

**You must not:**

- View download or share the imagery yourself or ask a pupil to share or download it. If you have already seen it you must tell the DSL
- Delete the imagery or ask the pupil to
- Ask the pupil to disclose any information regarding the imagery, this is the DSLs responsibility
- Share information about the imagery with anyone else, this includes staff, the pupils it involves or their parents and carers
- Say or do anything to blame or shame any young people involved
- You should explain that you need to report the incident, and reassure the pupil(s) that they will receive support and help from the DSL

**Initial review meeting**

Following a report of an incident, the DSL will hold an initial review meeting with appropriate school staff. This meeting will consider the initial evidence and aim to determine:

- Whether there is an immediate risk to pupil(s)
- If a referral needs to be made to the police and/or children's social care
- If it is necessary to view the imagery to safeguard the young person (in most cases, imagery should not be viewed)
- What further information is required to decide on the best response

DRAFT

- Whether the imagery has been shared widely and via what services and/or platforms (this may be unknown)
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the pupils involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved (in most cases parents should be involved)
- The DSL will make an immediate referral to police and/or children's social care if:
- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
- What the DSL knows about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the imagery is under 13
- The DSL has reason to believe a pupil is at immediate risk of harm owing to the sharing of the imagery (for example, the young person is presented as suicidal or self-harming)

If none of the above apply then the DSL, in consultation with the Head of School and other members of staff as appropriate, may decide to respond to the incident without involving the police or children's social care.

**Further review by the DSL**

If at the initial review stage, a decision has been made not to refer to police and/or children's social care, the DSL will conduct a further review.

They will hold interviews with the pupils involved (if appropriate) to establish the facts and assess the risks.

If at any point in the process there is a concern that a pupil has been harmed or is at risk of harm, a referral will be made to children's social care and/or the police immediately.

Informing parents:

The DSL will inform parents at an early stage and keep them involved in the process, unless there is a good reason to believe that involving them would put the pupil at risk of harm.

Referring to the police:

If it is necessary to refer an incident to the police, this will be done through a referral to the relevant police department in Kent or by calling 101.

Recording incidents:

All incidents involving sharing nudes or semi-nudes and the decisions made in responding to them will be recorded on CPOMS Safeguarding used at The Beacon.

## 24. Prevent and Radicalisation

The school recognises its duty to protect our pupils from indoctrination into any form of

DRAFT

extreme ideology which may lead to the harm of self or others. This is particularly important because of the electronic information available through the Internet. The school will aim, therefore, to do the following:

- Ensure all staff complete Prevent training every 2 years – National College

- Educate pupils on the appropriate use of social media and the dangers of downloading and sharing inappropriate material including that which is illegal under the Counter-Terrorism Act.

- Ensure that pupils are unable to access any inappropriate internet sites whilst using the school computers/laptops using appropriate filtering, firewalls and security settings.

- Educate pupils through lessons and assemblies on the concepts of radicalisation and extreme ideology.

- Inform pupils on the importance of Internet Safety both through the ICT curriculum and PHSE education.

Linking the teaching with relevant school policies, including those on sex and relationships education, online/e-safety, anti-bullying and child protection helps to ensure clear links with the whole school ethos.
MAST SG Team are required to remain updated in regard to current information and training. MAST SG Team will inform wider school staff of any updates in this area.

**If you have any concerns about extremism**

If a child is not suffering or likely to suffer from harm, or in immediate danger speak to the DSL / DDSL first to agree to a course of action.

If in exceptional circumstances the DSL is not available, this should not delay appropriate action being taken.
Speak to a member of the senior leadership team and/or seek advice from local authority children's social care.
If outside of school hours and if appropriate you would complete a referral to the local authority children's social care directly.
Inform the DSL or DDSL as soon as practically possible after the referral.

Where there is a concern, the DSL will consider the level of risk and decide which agency to make a referral to. This could include Channel, the government's programme for identifying and supporting individuals at risk of being drawn into terrorism, or the local authority children's social care team.
The Department for Education also has a dedicated telephone helpline, 020 7340 7264, which school staff and governors can call to raise concerns about extremism with respect to a pupil. You can also email counter.extremism@education.gov.uk. Note that this is not for use in emergency situations.
In an emergency, call 999 or the confidential anti-terrorist hotline on 0800 789 321 if you:

- Think someone is in immediate danger
- Think someone may be planning to travel to join an extremist group
- See or hear something that may be terrorist-related

DRAFT

## 25. Further information on so-called 'honour based' violence

So-called 'honour-based' violence (HBV) encompasses crimes which have been committed to protect or defend the honour of the family and/or the community, including Female Genital Mutilation (FGM), forced marriage, and practices such as breast ironing. All forms of so-called HBV are abuse (regardless of motivation) and should be handled and escalated as such. If in any doubt, staff should speak to the Designated Safeguarding Lead. Professionals in all agencies, and individuals and groups in relevant communities, need to be alert to the possibility of a child being at risk of HBV, or already having suffered HBV.

## 26. Mental Health

The school recognises the link between mental health and safeguarding. Staff are trained to identify signs of mental health difficulties that may indicate abuse, neglect, or exploitation. The Mental Health Lead works in partnership with the DSL to ensure appropriate support and referrals are made, including referrals to CAMHS or Early Intervention services.

Staff should be alert to signs of emotional distress, self-harm, suicidal ideation and mental ill health. Whilst mental health difficulties are not safeguarding concerns in isolation, they may indicate that a pupil is suffering, or is at risk of suffering, abuse, neglect or exploitation.

Any concerns for pupils should be logged immediately by staff on CPOMS.
This can then be triaged by both the safeguarding and mental health leads to ensure the correct advice and support can be offered as swiftly as possible

## 27. Online Safety (e–Safety)

An identified teacher, Samantha Barnes supported by a member of MAST, Julie Howell, has been given authority for Online- Safety throughout The Beacon and cascading the latest information.

The Beacon and Kent County Council believe that the safe use of information and communication technologies in schools and education settings brings great benefits. Recognising online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

This document has been developed alongside the work of the KSCMP Online Safety (e-Safety) Strategy Group.

**Creating an Online Safety Ethos - aims and policy scope**

DRAFT

- The Beacon believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- The Beacon identifies that the Internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- The Beacon has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. The Beacon also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.
- The purpose of The Beacon Online Safety Policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that The Beacon is a safe and secure environment.
    - Safeguard and protect all members of The Beacon community online.
    - Raise awareness with all members of The Beacon community regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff ', in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off site, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

**Writing and reviewing the online safety policy**

- The Beacon Online Safety Policy has been written by the school, involving staff, pupils and parents/carers, building on the KCC online safety policy template with specialist advice and input as required.
- The policy has been approved and agreed by the leadership and governing body
- The school has appointed a member of the Governing Body to take lead responsibility for online safety (e-Safety)
- The school has appointed a member of the leadership team as the online safety lead - Mr. Ady Young – Executive Head and Casey Fletcher – Head of School
- The school's online safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

- The School Online Safety (e-Safety) Coordinators are Julie Howell and Samantha Barnes
    - The School Designated Safeguarding Leads (DSL) are Julie Howell/ Casey Fletcher.
    - There is a School Online Safety (e-Safety) lead for the Governing Body.

DRAFT

- The date for the next policy review is September 2027

**Key responsibilities of the school/setting management team are:**

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practices to identify strengths and areas for improvement.
- Supporting online safety (e-Safety) leads in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensure that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of Schools systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (e-Safety lead)
- Governing Body and SLT will formally review filtering and monitoring annually as documented in KCSIE '2026'
- Key responsibilities of the Designated Safeguarding/Online Safety Lead Lead DSL Mr. Ady Young – Executive Head and Casey Fletcher – Head of School

**Lead DSL and Sam Barnes Online safety Lead**

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up to date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

DRAFT

- Work with the school/setting lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school leadership team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.
- Meet annually with the governor/board/committee member with a lead responsibility for online safety

**Key responsibilities of staff are:**

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

**Additional responsibilities for staff managing the technical environment are:**

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and Lead DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse is reported to the Headteacher.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the Safety Incident Log, and appropriate action is taken as advised.

DRAFT

- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaise with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

**Key responsibilities of children and young people are:**

- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.

**At a level that is appropriate to their individual age, ability and vulnerabilities:**

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.

**Key responsibilities of parents and carers are:**

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

**Emerging Online Harm Risks**

- **AI-generated harmful content**

DRAFT

Children may access AI-powered tools which can produce misleading, harmful or inappropriate content. Staff should be aware that AI can be used to:

- Generate realistic but false images, videos or information.
- Produce harmful advice or unsafe content.
- Facilitate bullying, harassment or exploitation.
- Create fake identities to deceive and groom children.
-

Pupils will be educated about the safe, responsible and critical use of AI technologies and how to verify information obtained online.

- **Deepfakes**

Deepfakes are digitally created or manipulated images, audio recordings or videos which appear genuine. These may be used to:

- Embarrass, bully or humiliate others.
- Create sexually explicit imagery.
- Spread misinformation.
- Damage reputations.
-

Any concerns involving manipulated imagery will be treated as a safeguarding concern and managed in accordance with child protection procedures.

- **Misinformation and Disinformation**

Children may encounter false or misleading information online.
The Beacon will support pupils to:

- Evaluate information critically.
- Identify trustworthy sources.
- Recognise manipulated content.
- Understand how algorithms can influence online experiences and beliefs.

- **Online challenges**

Staff will remain vigilant regarding online challenges, trends and viral content which may place children at risk of physical, emotional or psychological harm. Concerns regarding participation in harmful online activities will be reported to the Designated Safeguarding Lead (DSL).

- **Livestreaming risks**

The school recognises that live broadcasting platforms can expose children to:

- Inappropriate contact from adults.
- Pressure to engage in unsafe behaviours.

DRAFT

- Sharing of personal information.
- Exposure to harmful or illegal content.

Pupils will be taught how to use livestreaming and communication platforms safely and responsibly.

These are increasingly referenced within current safeguarding training conversations

**Online Communication and Safer Use of Technology. Managing the school/setting website**

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- Pupils' work will only be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website.

**Publishing images and videos online**

- The school will ensure that all images are used in accordance with the school image use policy.
- In line with the school's image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

**Managing email**

- Pupils may only use school/setting provided email accounts for educational purposes.
- All members of staff are provided with a specific school/setting email address to use for any official communication.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.

DRAFT

- Whole class or group email addresses may be used for communication outside of the school (in early years, infant and primary schools).
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

**Official videoconferencing and webcam use**

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school website.
- The equipment will be kept securely and if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Staff will ensure that external videoconferences are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

**Users**

- Pupils will ask permission from a teacher before making or answering a video conference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability. (schools should list how this will be enforced and achieved)
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

**Content**

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given, and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third-party intellectual property rights.
- The school will establish dialogue with other conference participants before taking

DRAFT

part in a video conference. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

**Appropriate and safe classroom use of the internet and associated devices**

- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Pupils will use age and ability appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access, and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability:

    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasionally directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools, and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
    - Secondary, sixth form and college pupils will be appropriately supervised when using technology, according to their ability and understanding.
    - In residential provisions the school will balance children's ability to take part in age-appropriate peer activities online with the need for the school to detect abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age-appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole school/setting requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending them for use at home.

**Management of school learning platforms/portals/gateways – LP (Learning Platform)**

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all

DRAFT

areas, in particular message and communication tools and publishing facilities.

- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the LP for the user may be suspended.
  d) The user will need to discuss the issues with a member of leadership before reinstatement.
  e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

## Social Media

### General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of The Beacon community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of The Beacon community will be encouraged to engage in social media in a positive, safe and responsible manner always.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of The Beacon community.
- All members of The Beacon community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupils and staff access to social media and social networking sites whilst on site and using school provided devices and systems
- The use of social networking applications during school hours for personal use is/is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of The Beacon community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and

DRAFT

safeguarding/child protection.

**Official use of social media**

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher.
- Official school social media channels will be set up as distinct and dedicated social media sites or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the school will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official school social media sites/channels in accordance with school/parent permissions.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Leadership Teams.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and pupils will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.
- The Beacon has an official Facebook Page for sharing school information with parents.
- Public communications on behalf of the school will, where possible, be read and agreed to by at least one other colleague.
- The school social media account will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

**Staff official use of social media**

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to always be professional and that they are an ambassador for the school.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest always and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright,

DRAFT

data protection as well as equalities laws.

- Staff must ensure that any image posted on the school social media channel has appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the school online safety (e-Safety) lead and/or the Headteacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and should communicate via school communication channels.

**Staff personal use of social media**

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/ member of Leadership Team/Head of School.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels - School email. Staff must not use personal accounts or information to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the school's Designated Safeguarding Lead.
- Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with school policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications

DRAFT

technology, including emails or social networking sites conflicts with their role in the school/setting.

- Members of staff are encouraged not to identify themselves as employees of The Beacon on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members and the wider school community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

**Pupils use social media**

- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

**Use of Personal Devices and Mobile Phones - Rationale regarding personal devices and mobile phones**

- The widespread ownership of mobile 'phones and a range of other personal devices among children, young people and adults will require all members of The Beacon community to take steps to ensure that mobile 'phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the school Acceptable Use Policy.
- The Beacon recognises that personal communication through mobile technologies is

DRAFT

an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.
- The school aims to minimise unnecessary mobile phone use during the school day and will maintain clear procedures regarding pupil and staff mobile phone use in line with safeguarding and behaviour expectations

**Expectations for safe use of personal devices and mobile phones**

- Electronic devices of all kinds that are brought in to school are always the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile 'phones and personal devices are not permitted to be used in certain areas within the school site, such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile 'phones or personal devices is forbidden by any member of the school community, and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Members of staff will be issued with a school/work 'phone number and email address where contact with pupils or parents/carers is required.
- All members of The Beacon community will be advised to take steps to protect their mobile 'phones or devices from loss, theft or damage.
- All members of The Beacon community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile 'phones and personal devices should not be shared.
- All members of The Beacon community will be advised to ensure that their mobile 'phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.
- School/setting mobile 'phones and devices must always be used in accordance with the Acceptable Use Policy
- School/setting mobile 'phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

**Pupils' use of personal devices and mobile 'phones**

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile 'phones.
- All use of mobile 'phones and personal devices by children will take place in accordance with the acceptable use policy.
- Mobile 'phones and personal devices will be handed to the class tutor at the start of the day and returned at the end of the day.

Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile 'phones or devices for a specific education purpose does not mean that blanket use is permitted.
If members of staff have an educational reason to allow children to use their mobile 'phones or personal devices as part of an educational activity, then it will only take place when approved by the Leadership Team.

DRAFT

If a pupil needs to contact his/her parents/carers they will be allowed to use a school ‘phone. Parents are advised not to contact their child via their mobile ‘phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher.
Pupils should protect their phone ‘numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile ‘phones and personal devices and will be made aware of boundaries and consequences.
‘Phones and devices must not be taken into examinations. Pupils found in possession of a mobile ‘phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil’s withdrawal from either that examination or all examinations.
If a pupil breaches the school policy, then the ‘phone or device will be confiscated and will be held in a secure place in the school office. Mobile ‘phones and devices will be released to parents/carers in accordance with the school policy.
School staff may confiscate a pupil’s mobile ‘phone or device if they believe it is being used to contravene the school’s behaviour or bullying policy. The ‘phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer. Searches of mobile ‘phone or personal devices will be carried out in accordance with the school’s policy.
If there is suspicion that material on a pupil’s personal device or mobile ‘phone may be illegal or may provide evidence relating to a criminal offence, then the device will be handed over to the police for further investigation.

**Staff use of personal devices and mobile ‘phones**

- Members of staff are not permitted to use their own personal ‘phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with leaders/managers.
- Staff will not use personal devices such as mobile ‘phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile ‘phones and devices will be switched off/switched to ‘silent’ mode during lesson times.
- Bluetooth or other forms of communication should be “hidden” or switched off during lesson times.
- Personal mobile ‘phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile ‘phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school/setting policy, then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile ‘phone or personal device or have committed a criminal offence, then the police will be contacted, and allegations will be responded to by following the allegations management policy.

**Visitors use of personal devices and mobile phones**

- Parents/carers and visitors must use mobile ‘phones and personal devices in

DRAFT

accordance with the school's policy.

- Use of mobile 'phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

**Policy Decisions - Reducing online risks**

- The Beacon is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit, and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the Online Safety (e–Safety) Policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the school's leadership team.

**Internet use throughout the wider school/setting community**

- The school will liaise with local organisations to establish a common approach to online safety (e–Safety).
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

**Authorising Internet access**

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff; pupils and visitors, will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the school community (such as with children with special educational needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

**Engagement Approaches - engagement and education of children and young people**

- Online safety (e-Safety) will be taught with ICT/Computing lessons and through

DRAFT

digital technology curriculum, to raise awareness regarding the importance of safe and responsible Internet use amongst pupils.

- Education about safe and responsible use will precede internet access.
- Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- The pupil Acceptable Use expectations and posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

**Engagement and education of children and young people who are considered to be vulnerable**

- The Beacon is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

**Engagement and education of staff**

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- To protect all staff and pupils, the school will implement Acceptable Use Policies which highlight appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

DRAFT

**Engagement and education of parents and carers**

- The Beacon recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the Internet and digital technology.
- Parents' attention will be drawn to the School Online Safety (e-Safety) Policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well-attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of ways.
- Parents will be encouraged to role model positive behaviour for their children online.

**Managing Information Systems - managing personal data online**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Full information regarding the school's approach to data protection and information governance can be found in the school's information security policy.

**Security and Management of Information Systems**

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off the site should be stored securely. Staff are advised to use OneDrive as a preferred system to store data.
- Portable media may not be used without specific permission followed by an anti-virus /Malware scan. Staff are advised to use OneDrive as a preferred system to store data.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's TDrive will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices

**Password policy**

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password

DRAFT

private.
- From year 1, all pupils are provided with their own unique username to access school systems. Accounts are created and details sent to class teachers.
- We require staff and pupils to use strong passwords for access into our system.
- We require staff and pupils to change their passwords regularly to ensure their accounts remain safe.

**Filtering Decisions**

- The school's Internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- The school uses educational filtered secure broadband connectivity through the school which is appropriate to the age and requirement of our pupils.
- The school uses Smoothwall filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.
- The school will work with KCC and the school's broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school Headteacher or Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The school filtering system (Smoothwall) is a member of Internet Watch Foundation and will block all sites on the (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

**Management of applications (apps) used to record children's progress**

- The Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainments or photographs.
- Only school issued devices will be used for apps that record and store children's personal details, attainments or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

**Responding to Online Incidents and Concerns**

DRAFT

- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e- Safety) incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Multi-Agency Partnership thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Complaints about online bullying will be dealt with under the school's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the head teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the schools complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team (LESAS) or Kent Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team (LESAS).
- If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Team (LESAS) to communicate to other schools/settings in Kent.

- Parents and children will need to work in partnership with the school to resolve issues.

**Procedures for Responding to Specific Online Incidents or Concerns**

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventually so professional judgement and support from appropriate agencies such as The Education People, Police, CSET and Children's Social Care is encouraged.
Some settings may not feel that these sections are relevant due to the age and ability of

DRAFT

children; however, it is recommended that designated safeguarding leads ensure that their settings safeguarding policies and procedures are robust and are applicable for a range of safeguarding issues should they occur.
Some schools and settings will place these sections within existing safeguarding and child protection policies and procedures rather than the online safety policy or within other appropriate policies and procedures. Other settings will prefer to keep this content as reference material for Designated Safeguarding Leads.

**Responding to concerns regarding Online Child Sexual Abuse**

- The Beacon will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The Beacon views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads – Julie Howell/Casey Fletcher
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team (LESAS) and/or Kent Police.
- If the school are made aware of incident involving online child sexual abuse of a child, then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform Kent police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

- The school will act regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted, then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguard their community.
- The school will ensure that the Click CEOP report button is visible and available to

DRAFT

pupils and other members of the school community, for example including the CEOP report button on the school website homepage.

**Responding to concerns regarding Indecent Images of Children (IIOC)**

- The Beacon will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will act regarding Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed; then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school/setting are made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Multi-Agency Partnership procedures.
  - Immediately notify the school Designated Safeguarding Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LESAS (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the Internet, then the school will:
  - Ensure that the Designated Safeguarding Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school is made aware that indecent images of children have been found on the school's electronic devices then the school will:
  - Ensure that the Designated Safeguarding Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguarding Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved

DRAFT

until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

**Responding to concerns regarding radicalisation or extremism online**

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which considers the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately, and action will be taken in line with the school safeguarding policy.

**Responding to concerns regarding cyberbullying**

- Cyberbullying, along with all other forms of bullying, of any member of The Beacon community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

**Online Safety and the 4 Cs**

The Beacon recognises that technology is a significant component of many safeguarding and wellbeing issues. Our approach to online safety considers the 4 Cs of online risk: Content, Contact, Conduct and Commerce.

DRAFT

Staff will remain alert to:

- **Content:** Children being exposed to illegal, inappropriate or harmful content, including misinformation, pornography, racism, misogyny, self-harm, suicide, eating disorders, radicalisation and extremism.
- **Contact:** Harmful online interaction with other users, including peer-to-peer pressure, inappropriate commercial advertising and adults posing as children or young people with the intention of grooming or exploiting them.
- **Conduct:** Online behaviour that increases the likelihood of, or causes, harm, including the sharing of explicit images, online bullying and inappropriate or harmful use of technology.
- **Commerce:** Risks associated with online gambling, inappropriate advertising, phishing and other financial scams.

Online safety will be embedded within The Beacon's wider safeguarding practice. This will include staff training, appropriate filtering and monitoring arrangements, age-appropriate education for children, clear procedures for responding to concerns, and effective communication with parents and carers.
Staff will recognise that online and offline safeguarding concerns are often interconnected and will respond to online safety concerns in accordance with the setting's safeguarding and child protection procedures.

DRAFT

## 28. Appendix One – Indicators of Abuse

**INDICATORS OF NEGLECT**

Neglect is not always easy to recognise, but the following may give cause for concern:

- Consistent hunger
- Poor hygiene
- Inappropriate dress
- Consistent lack of supervision, especially in dangerous activities for long periods
- Unattended physical problems or medial needs
- Abandonment

**BEHAVIOURAL INDICATORS OF NEGLECT**

- Begging
- Stealing food
- Extended stay at playground or school
- Constant fatigue, listlessness
- Poor relationship with caregiver

**INDICATORS OF EMOTIONAL ABUSE**

The signs of emotional abuse are probably the hardest to link to actual abuse as there may be other factors affecting the young person's/adults' behaviour or physical development; however, we have compiled a list of the main indicators:

**PHYSICAL INDICATORS OF EMOTIONAL ABUSE**

- Failure to thrive
- Delays in physical development or progress

**BEHAVIOURAL INDICATORS OF EMOTIONAL ABUSE**

Behavioural disturbances such as (particularly if they are new behaviours):

- Sucking, biting, rocking, anti-social, destructive sleep disorders, inhibition of play
- Compliant, passive, aggressive, demanding
- Low self-esteem

**INDICATORS OF SEXUAL ABUSE**

The signs of **sexual abuse** are varied and can often be linked with other forms of abuse. The following list is, as always, only a guide and cannot be relied on as exhaustive. They too can be sub-divided into two groups.

**Physical Indicators**

- Difficulty in walking, sitting down
- Stained or bloody underclothing
- Pain or itching in genital area
- Bruising, bleeding, injury to external genitalia, vaginal and/or anal areas

DRAFT

- Vaginal discharge
- Bed-wetting
- Excessive crying
- Sickness

**Behavioural Indicators**

- Bizarre, sophisticated or unusual sexual behaviour or knowledge
- Promiscuity
- Sudden changes in behaviour. Cut off from body sensations (e.g. delayed reaction to pain)
- Running away from home
- Wary of adults
- Feeling different from other young people/adults
- Unusual avoidance of touch
- Reporting of assault
- Substance abuse (e.g. glue sniffing)
- Emotional withdrawal through lack of trust in adults
- Over compliance with requests of others
- Frequent complaints of unexplained abdominal pains
- Eating problems
- Sleep disturbances
- Poor peer relationships
- Possessing money or "gifts" that cannot be adequately accounted for

**PHYSICAL ABUSE**

Physical Indicators
Unexplained bruises/welts/lacerations/abrasions:

- On face, lips, mouth
- On torso, back, buttocks, thighs
- In various stages of healing
- Clustering forming regular patterns
- Reflecting shape of article used, e.g. belt, buckle, electrical flex
- On several different surface areas
- Regularly appear after absence, weekend, or holiday
- Bite marks or fingernails marks

**Unexplained burns:**

- Cigarettes burn especially on soles, buttocks, palms or back
- "Immersion" burns, where hands feet or body have been forcibly immersed in very hot water
- Patterns like electrical burners, iron, etc.
- Rope burns on arms, legs, neck or torso

**Unexplained fractures:**

- To skull, nose, facial structure
- In various stages of healing
- Multiple or spiral fractures

DRAFT

**Behavioural indicators of physical abuse:**

- Flinching when approached or touched
- Reluctance to change clothes for P.E. lessons
- Wary of adult contact
- Difficult to comfort
- Apprehension when other children cry
- Crying/irritability
- Frightened of parents
- Afraid to go home
- Rebelliousness in adolescence
- Reported injury caused by parents
- Behavioural extremes - aggressiveness, withdrawal, impulsiveness
- Regression to child-like behaviour
- Apathy
- Depression
- Poor peer relationships
- Panic in response to pain
- Low self esteem
-

**Online Safety Risks:**

Misinformation

Disinformation
Conspiracy theories
AI generated content
Deep-fake imagery
Nudification technologies

DRAFT

**Update Schedule**

| Version | Reviewed | Reason for Update | Next review date | Governor agreement |
|---|---|---|---|---|
| 1 | March 2024 | Updates to staff | September 2024 | Agreed by Governors May 2024 |
| 2 | September 2025 | Annual review and updates to staff and relevant guidance | September 2026 | Agreed by Governors 10.10.2025 |
| 3 | September 2026 | Annual review and updates to staff and relevant guidance | September 2027 | |

DRAFT

## Policy Enhancements for Full Statutory Compliance

**Safeguarding Young Adults (18–25)**

In accordance with the Care Act 2014, this policy extends safeguarding responsibilities to young adults aged 18–25, particularly those with Education, Health and Care Plans (EHCPs) or transitioning from children's to adult services. Staff must be aware of the specific vulnerabilities and safeguarding needs of this age group, including mental capacity, consent, and access to adult safeguarding services. The DSL will liaise with adult social care where appropriate.

**Low-Level Concerns and Whistleblowing**

In line with Part Four of Keeping Children Safe in Education (KCSIE) 2026, all staff must report any low-level concerns about adults working with children, even if they do not meet the harm threshold. These concerns may include inappropriate conduct, boundary breaches, or behaviour inconsistent with the staff code of conduct. Reports should be made to the DSL or Headteacher and recorded confidentially. The school maintains a low-level concerns log and ensures staff are trained to recognise and report such concerns.

**Filtering and Monitoring Responsibilities**

To comply with KCSIE 2026, the school has clearly defined roles and responsibilities for filtering and monitoring online activity. The Headteacher oversees the effectiveness of filtering systems, while the Online Safety Lead and technical staff are responsible for implementing and reviewing filtering and monitoring tools. Regular audits are conducted to ensure systems are age-appropriate, effective, and aligned with safeguarding needs. Any breaches or concerns are reported to the DSL and recorded in the online safety log.

DRAFT