
# Safeguarding Children and Young Persons Policy including Online Safety (e-safety)

Update Schedule

| Version | Reviewed | Reason for Update | Next review date | Governor agreement |
|---|---|---|---|---|
| 1 | Oct 16 | Revised/transfer | Oct 17 | With Gov for agreement |
| 2 | March 17 | Revised updated as per requirements | Oct 17 | Agreed with chair of Governors 20/03/17. |
| 3 | May 2017 | Revised updated as per requirements | Oct 17 | Agreed 22.5.17 |
| | | | | |
| | | | | |
| | | | | |

**Safeguarding Children and Young Persons Policy**

## 1.0 Safeguarding Children & Young Person 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.

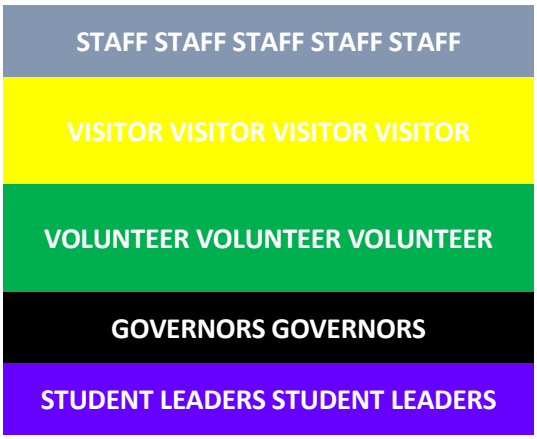
**The Beacon Folkestone, through the embedding of its Core Values, will ensure that all children and young people have the same protection regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity. The Beacon Folkestone is committed to anti-discriminatory 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 Folkestone but also in the wider community.

Ensuring that the Safeguarding Policy is updated as and when required is the responsibility of the Designated Safeguarding Leads, the identifiable individual is the Head of Business and Development, in his/her absence it becomes the responsibility of The Multi Agency Leader and the Safeguarding Governor.

**1.1 Identifying adults that access the school (not including NHS/Health Departments)**

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




Staff directly employed by The Beacon
**Access all area**
Visitors - Including maintenance/people on courses/people accessing the café
**Escorted by Paid Adults**
Any adult working at The Beacon not in a paid capacity
**Can only access the areas they volunteer in**
**The school governors can access the non-pupil areas of the school**
**Student leaders are usually accompanied by a staff member**

**Our NHS and Health colleagues do not have electronic access to the school.**

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

2.0

<table>
<tr><td colspan="2">  <br>Ady Young<br>Head of Support and Development<br>DSL Lead</td><td colspan="2">  <br>Tanya Lees<br>Head of School<br>Deputy DSL</td></tr>
<tr><td>Irene White<br>Assistant Head<br>Deputy DSL</td><td>  </td><td>Paul Woods<br>Teacher<br>Deputy DSL</td><td>  </td></tr>
<tr><td>Claire Lucas<br>Multi Agency Officer<br>Deputy DSL</td><td>  </td><td>Mel Winter<br>Assistant Head<br>Deputy DSL</td><td>  </td></tr>
<tr><td>Lynda Evans<br>Assistant Head<br>Teacher - STLS<br>Deputy DSL</td><td>  </td><td colspan="2" rowspan="2">Colin Wimset<br>Safeguarding Governor<br>  <br>colin.wimsett@thebeacon.kent.sch.uk</td></tr>
<tr><td>Alison Kane<br>Multi Agency Officer<br>Deputy DSL</td><td>  </td></tr>
<tr><td>Jimmy Peters<br>Multi Agency Leader<br>Deputy DSL</td><td>  </td><td colspan="2"></td></tr>
</table>

**3.0 Legal Framework**

| | |
|---|---|
| Children's Act | 1989 |
| United Convention of the Right of the child | 1991 |
| Data Protection Act | 1998 |
| Human Rights Act | 1998 |
| Sexual Offences Act | 2003 |
| Children Act | 2004 |
| Safeguarding Vulnerable Groups Act | 2006 |
| Protection of Freedoms Act | 2012 |
| Children and Families Act | 2014 |
| Special Educational Needs and Disability (SEND) Code of Practice 0-25 years - Statutory Guidance for Organisations; which work with and support Children and Young People who have special educational needs or disabilities; HM Government | 2014 |
| DfE Child Sexual Exploitation | 2017 |
| HM Government Working Together to Safeguard Children | 2015 |
| DfE Keeping Children Safe in Education | 2016 |
| Working Together to Safeguard Children | 2015 |

**3.1 Supporting Policies**

Anti-Bullying Policy
Attendance Policy
Children in Care policy
CCTV Policy
Children's Rights Policy
Recruitment Policy
Whistle Blowing
Induction of New Staff Policy
Physical Intervention
Confidentiality, Privacy and Access to Pupil Files.
Collective Worship Policy
Drugs
Critical Incidence Policy
First Aid
Medication policy
Personal/Intimate Care
Pupil Safety on and off School Site Policy
School Security
Data Protection Policy

**3.2 Links to Other Agencies**

**Kent Safeguarding Children Board**

Room 2.60, 2nd Floor
Sessions House
County Hall
Maidstone
ME14 1XQ

**Email:** kscb@kent.gov.uk
**Tel:** 03000 421126

KSCB - Kent Safeguarding Children's' Board
http://www.kscb.org.uk/
NSPCC - National Society for the Prevention Cruelty to Children
https://www.nspcc.org.uk/

**4.0 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 students of all ages attend The Beacon Folkestone.
**Parent/Carers** refers to birth parents and other adults who are in a parenting role, for example step-parents, foster carers and adoptive parents.

**4.1 Aim**

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

**4.2 School policy, ethos and training**

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

We are committed from senior management and governors in the school to deal with the issue of child sexual exploitation … and ensure that any investigations ensure are supportive and appropriate.

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 Folkestone also display posters and distribute 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.

**4.3 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.

**5.0** Categories of Abuse (indicators included below)

- **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 individuals will (internet/mobile phones).
- **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.
- **Financial Abuse –** Theft of an individual's money, exploitation, pressure to make an 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.

**CATEGORIES OF CHILD/ADULT ABUSE**

Abuse can take on many forms but is usually divided into four categories:

- Neglect
- Emotional abuse
- Sexual abuse
- Physical abuse

**5.1 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

**5.2 BEHAVIOURAL INDICATORS OF NEGLECT**

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

**5.3 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:

**5.4 PHYSICAL INDICATORS OF EMOTIONAL ABUSE**

- Failure to thrive
- Delays in physical development or progress

**5.5 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.

**6.0 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.

**6.1 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.
- Vaginal discharge.
- Bed-wetting.
- Excessive crying.
- Sickness.

**6.2 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.

**7.0 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.

**7.1 Unexplained burns:**

- Cigar or cigarette burns 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 burner, iron etc.
- Rope burns on arms, legs, neck or torso.

**7.2 Unexplained fractures:**

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

**7.3 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.

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

Whilst any of the above indicators may identify that abuse is occurring or has occurred, some of them may have other causes. Causality is particularly important when pupils have social and communication problems associated with autism or specific medical problems. Some children/young people display specific indicators of abuse at all times and where these have been shown not to be as a result of abuse it is important to monitor changes in a child's/young person's behaviour, physical condition, emotional state and sociability. Such changes may themselves indicate that abuse is taking place.
Staff should read individual child's/young person's files to familiarise themselves with medical conditions that can present with the same symptoms as abuse. Such judgements often require sophisticated knowledge and understanding. Staff must err on the side of caution. *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.*

**If a child/young person chooses to talk to you and discloses that he/she has been abused.**
**Your role is to ensure that no further harm will take place.**

**BELIEVE THE CHILD/YOUNG PERSON AND IMMEDIATELY INFORM A DESIGNATED SAFEGUARDING LEAD**

**8.1 Key Safeguarding Personnel Across the Beacon**

- The Beacon Folkestone 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) and an on call system is in operation so that parents/staff can call a DSL until 7.30pm Monday to Friday.
- They keep written records of any concerns/investigations.
- Refer concerns/investigations to appropriate agencies (Social Services/Early Help/Police).
- Attends/contributes to Child Protection Conferences.
- Provides face to face Safeguarding Training to staff as part of their induction.
- Coordinates The Beacon Folkestone's policy on Child Protection procedures.
- Develops effective links to appropriate agencies.
- Is instrumental in updating Safeguarding Policy.
- Liaises with the nominated Safeguarding Governor.
- Informs staff of changes as soon as practically possible.
- Attends additional training as required.

**8.2 Governors Complete a Safeguarding Audit twice a year.**
**The findings are discussed at the next governing body meeting in way of a report - it must clearly state actions required and the lead person.**

**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<br>Report verbally and write, verbatim, what the c h i l d / 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:**

| | |
|---|---|
| 1 | They cannot find the words to say what is happening because of age, learning, language and hearing difficulties. |
| 2 | They do not have an adults' permission to tell and actual or implied threats have been used |
| 3 | They have found they cannot trust a parent or an adult who they believed they knew well. |
| 4 | They assume that they will not be believed. |
| 5 | They believe silence will help to protect others in their family. |
| 6 | They have been forced to take the blame for what is happening. |
| 7 | They do not know what the alternatives are or have access to agencies which can offer protection and/or help. |
| 8 | They are not yet ready to talk about their experience - they do not feel safe enough. |

**8.3 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 persons 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 Ofsted.

**8.4 Concerns involving members of staff**

- Any concerns that involve allegations against a member of staff **must** be referred immediately to the DSL who has to contact the LADO within 24 hours of the allegation being made.

- This may result in a consultation or a recommendation for a staff member being suspended.

- Should the allegation be against a DSL then the remaining DSL's will make a referral directly to the Safeguarding Team and LADO.

*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.*

**8.5 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.***

In the case of a clear disclosure or significant concern a Designated Safeguarding Lead must follow the Kent & Medway Safeguarding Children Procedures as follows;

- Consult with the Social Services Department
- And/or consult with the child's/young person's Safeguard Service
- Following consultation, advice will have been given on appropriate action. If a pupil is identified as being in need of protection, the school's DSL will formally refer to Social Services by phone following up with a completed Social Services Referral Form (you will receive an e-mail confirmation which must be attached to the child's/young person's paperwork
- Inform the Executive Head Teacher who will inform the Chair of Governors
- Inform the Safeguarding Governor in the first instance by phone and follow up with an e-mail.
-

**8.6 Contact with Parents/Guardians/Carers**

Staff in school are in a strong position to detect child/young person abuse. It is a highly emotive area which may cause an initial reluctance on the part of the school to take a course of action which would antagonise parents, particularly where the school has striven to create a good working relationship between home and school.

***However, the overwhelming criterion is the safety and well-being of the young people and this will over-rule any reluctance to act.***

**8.7 Inter-Agency Working and Confidentiality**

Early Help means providing support as soon as a problem emerges. This forms part of The Beacon Folkestone's Multi Agency approach to safeguarding procedures. Inter-Agency Working means that we are able to create a holistic assessment around the person and their family enabling those agencies involved to provide the correct support.

After referral, an early help assessment will be undertaken by a lead professional.

Confidentiality is of paramount importance; parents/carers will be informed where possible if we need to discuss sensitive information with other agencies. Sharing information can be essential in putting an appropriate plan of support around a pupil and their parent/carer.

**8.8 Preventative Education/Procedures**

The Beacon Folkestone 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 Folkestone will include specific teaching about the risks of child abuse 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 | FGM |
| Child Sexual Exploitation | CSE |
| Prevent Strategy | |
| On line safety | |
| Youth Produced Indecent Images | |

The Beacon Folkestone 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 as an induction.
- Training to parents/carers.
- Annual on-line certificated refreshers to all staff/Volunteers and Governors.
- Staff induction, completed in the first week of employment before staff work with the pupils

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 available to staff at all times.
Within the Beacon, the Multi Agency Support Team (MAST) have literature to help staff in the safeguarding of the pupils. Staff are able to seek guidance from any DSL throughout the Beacon.

**8.9 Child Abuse by Another Child**

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.

**8.10 Bullying**

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

**8.11 Record Keeping – Child/Adult Protection**

It is vital that the school keeps accurate and detailed records of all concerns relating to safeguarding and child protection matters for a variety of reasons:

A member of staff may have a concern about a particular child/young person, but not feel that it is important enough to act upon. That concern may stay in the back of the staff member's mind, and increase anxiety and stress-related responses on a day-to-day basis. If the concern is recorded in a matter of fact manner, and the responsibility for it handed on to the DSL, the staff member is freed from this anxiety, and also in a position to discuss further concerns with the DSL should they arise.

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.

**The records serve as a database for future decisions.**

"Be prepared to think the unthinkable and
Believe the unbelievable"
Ray Wyre Gracewell Clinic 1987

**8.12 Female Genital Mutilation (FGM)**

In April 2014 every school in England received new safeguarding guidelines and detailed information on identifying and responding to Female Genital Mutilation.

FGM is a procedure carried out on young girls between the ages of infancy and 15 years of age.

Female Genital Mutilation is classified as a form of Child Abuse in the UK. It therefore makes the procedure of it a serious Child Protection issue.

It is illegal for anyone to perform FGM in the UK or to arrange for a child to be transported to another country for the procedure. The maximum sentence for carrying out FGM or helping it to take place is 14 years in prison.

Staff across The Beacon Folkestone receive face to face training on FGM as part of their induction package, including how to report record concerns. There is a mandatory refresher annually.

There is lots of information and support available online for parents/carers concerned about this subject or if you know someone who is at risk, training sessions are offered to parents twice a year.

**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/

**8.13 Child Sexual Exploitation**
We believe that at The Beacon Folkestone we are well placed to teach pupils how to make positive choices and informed decisions in their relationships so that they can protect themselves from sexual 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 Folkestone 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 regards to Child Sexual Exploitation, safeguarding underpins their Core Values. Staff advocate appropriately for the pupils and their families.

**8.14 Youth Produced Indecent Images is a child protection issue**
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 Youth Produced Indecent Images as part of their e-safety education. The School takes incidences of Youth Produced Indecent Images extremely seriously, and deals with them in accordance with child protection procedures, including reporting to the police.

**8.15 Prevent and Radicalisation**
The School recognises its duty to protect our pupils from indoctrination into any form of 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 therefore aim to do the following:

- 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 through the use of 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, e-safety, anti-bullying and child protection helps to ensure clear links with the whole school ethos.

MAST are required to remain updated in regards to training.

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 the 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.

**8.16 Actions**
If staff have a concern regarding a child that might be at risk of HBV, they should activate local safeguarding procedures, using existing national and local protocols for multi-agency liaison with police and children's social care.

**8.17 Recording**
The process for recording of concerns operated at The Beacon Folkestone is

| | | |
|---|---|---|
| Pink | Safeguarding Concern Form | Staff use this form if they believe the incident has a safeguarding implication and they feel that there **is** a requirement for further investigation. |

**There is a Pupil Friendly Safeguarding Poster placed around the school.**

**A Parent Friendly Safeguarding Policy is sent home annually and available on our website.**

**References are made to the document**
**Keeping Children Safe in Education Policy 2016**

## 9.0 Online Safety (e–Safety)

Kent County Council believes 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 Policy template will help schools and settings to form an online safety (or 'e-Safety') policy that is appropriate to their needs and requirements.
This document only contains the policy template for schools and settings and must be read in conjunction with the guidance document.
This document has been the work of the KSCB Online Safety (e-Safety) Strategy Group.

### *9.1 Creating an Online Safety Ethos*

#### *Aims and policy scope*

- 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 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).

### *9.2 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), Mr Colin Wimsett.
- The school has appointed a member of the leadership team as the online safety lead- Multi Agency Lead, Mr Ady Young
- The Schools 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 MAST.
- The School Designated Safeguarding Lead (DSL) is Mr Ady Young
- The School Online safety (e-Safety) lead for the Governing Body is Colin Wimsett
- The date for the next policy review is March 2018

### *9.3 Key responsibilities of the community*

***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 practice to identify strengths and areas for improvement.
- Supporting the online safety (e-Safety) lead 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 ensuring 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 regarding 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).

***9.4 Key responsibilities of the designated safeguarding/online safety lead is Mr Richard Fairhall – IT Teacher***

- 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.
- 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 management 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 regularly with the governor/board/committee member with a lead responsibility for online safety

***9.5 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 to 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.

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

- Providing a safe and secure technical infrastructure which support 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 DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising 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.

***9.7 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.

***9.8 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.

10.0 ***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 Executive Head Teacher 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.

***10.1 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 Schools image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

***10.2 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 the Lead Designated Safeguarding Lead if they receive offensive communication, this will then be recorded and investigated accordingly.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- 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.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

***10.3 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 videoconference 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.

**10.4 Users**

- Pupils will ask permission from a teacher before making or answering a videoconference 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 in writing prior to children taking part in videoconferences.
- Video conferencing 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.

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

***10.6 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 occasional 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.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure 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 for use at home.

***10.7 Management of school learning platforms/portals/gateways***

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

***11.0 Social Media Policy***

***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 at all times.
- 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 accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

***11.1 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 Head of School.
- Official school social media channels will be set up as distinct and dedicated social media site 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.
- Members of staff running official school social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- 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 1998, 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 the school image use policy.

- 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.
- 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 does not have an* official social media channels
- All parent/carer letters and communications will be agreed by SLT prior to sending.
- 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.

### *11.2 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 be professional at all times 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 at all times 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, data protection as well as equalities laws.
- Staff must ensure that any image posted on the school social media channel have 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 Executive Head Teacher 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 using social media officially will sign the school social media Acceptable Use Policy before official social media use will take place.

### *11.3 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 make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head of School/manager.
- Any communication from pupils/parents received on personal social media accounts will be reported to the schools 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 Schools 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 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 also 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, this could result in a disciplinary procedure.
- School email addresses will not be used for setting up personal social media accounts.

***11.4 Pupils use of 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.
- Pupils should not use their mobile phones to take photos of other pupils during the school day.

***11.5 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 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 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.

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

- Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. 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.

**11.7 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 into the class tutor at the start of the day and returned at the end of the day, with the exception of 6th from students devices which will be switched off and kept out of sight during classroom lessons and while moving between lessons.

- 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.
- 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 Head of School.
- 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 Schools 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 Schools 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.

**11.8 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-exiting 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 responding to following the allegations management policy.

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

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the Schools 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.

***12.0 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 Schools leadership team.

***12.1 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

***12.2 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 education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

***13.0 Engagement Approaches***

***Engagement and education of children and young people***

- Online safety (e-Safety) will be taught with ICT/Computing lessons and during Tutor time, 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 Schools 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.

### *13.1 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).

### *132 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 highlights 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 is 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 monitor 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.

### *13.3 Engagement and education of parents and carers*

- The Beacon recognise 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 formats.
- Parents will be encouraged to role model positive behaviour for their children online.

***14.0 Managing Information Systems***

***Managing personal data online***

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Full information regarding the schools approach to data protection and information governance can be found in the Schools information security policy.

***14.1 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 site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network 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

**14.2 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 private.
- From year 1, all pupils are provided with their own unique username to access school systems.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff and pupils to change their passwords every year.

***14.3 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 KPSN which is appropriate to the age and requirement of our pupils.

- The school uses Light Speed 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 Schools 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 Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (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.

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

- The Head of School/manager 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, attainment or photographs.
- Only school issued devices will be used for apps that record and store children's personal details, attainment 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.

***14.5 Responding to Online Incidents and Concerns***

- 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 Board 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 Executive 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 will 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 Safeguards Team 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.
- If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

### *14.6 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 eventuality so professional judgement and support from appropriate agencies such as the Education Safeguarding Team, 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 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.

### *14.7 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Youth Produced Indecent Images")*

- The Beacon ensure that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating indecent images of children (known as "Youth Produced Indecent Images").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The Beacon views "Youth Produced Indecent Images" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead Mr Ady Young.
- If the school are made aware of incident involving indecent images of a child 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 the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children 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.
- Implement appropriate sanctions in accordance with the Schools behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The school will not view the image unless there is a clear need or reason to do so.
- The school will not send, share or save indecent images of children and will not allow or request children to do so.

- If an indecent image has been taken or shared on the school/settings network or devices, then the school will take action to block access to all users and isolate the image.
- The school will need to involve or consult the police if images are considered to be illegal.
- The school will take action regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Youth Produced Indecent Images' in schools: advice and support around self-generated images. What to do and how to handle it".
- The school will ensure that all members of the community are aware of sources of support.

***14.8 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 Lead Mr Ady Young.
- 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 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 take action 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 safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

### *14.9 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 take action regarding of 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 access accidental access to of 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 Boards procedures.
    - Immediately notify the school Designated Safeguard 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 LADO (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 Safeguard 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 are made aware that indecent images of children have been found on the Schools electronic devices, then the school will:
    - Ensure that the Designated Safeguard 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 Safeguard 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 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.

***14.10 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 takes into account 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.

***14.11 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 schools 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 schools 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.

15.0 **The Beacon Equality Statement**

The Beacon Folkestone is committed to ensuring equality of opportunity to all pupils, staff and visitors. Our Core Values are at the foremost of everything we do and we ensure all at The Beacon are treated equally regardless of age, disability, race, colour, ethnicity, nationality, religious belief, gender, gender identity, transgender, sexual orientation or marital status.
The Beacon strives to be an all-inclusive environment and is always looking for opportunities to broaden the knowledge and experiences of everyone who is involved with both our services, and the staff and clients of those using the services of our multi-agency hub.
Our aims for this year are to ensure there are more equal opportunities for pupils, staff, their families and the wider community, regardless of their disability and this forms an integral part of our School Improvement Plan.
The aims for 2016-2019 are to build and improve schemes to help bring down barriers for disabled children and young people and to broaden the experience of life both inside and outside the school community for all staff & pupils.