SAFEGUARDING POLICY
Incorporating our Child Protection Policy, Safer Recruitment Policy, E-Safety Policy and 'Sexting' Policy

SCHOOL STATEMENT

Safeguarding and promoting the welfare of children is defined for the purposes of this policy as protecting children from maltreatment; preventing impairment of children's health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.

The terms 'child' and 'children' includes everyone under the age of 18.

The Governors and Trustees take seriously their responsibility to protect and safeguard the welfare of children and young people entrusted to the school's care. The Governors and Trustees will ensure that persons with leadership and management responsibilities at the school demonstrate good skills and knowledge appropriate to their role and fulfil their responsibilities effectively so that the independent school standards are met consistently; and actively promote the well-being of pupils according to section 10(2) of the Children Act 2004(**a**).

The Vine Christian School is a Safeguarding School. We will invoke Child Protection Procedures where necessary.

Our Designated Safeguarding Lead is Mrs Johanna Esterhuizen. Her role is to provide support and direction to staff members to carry out their safeguarding duties and to liaise closely with other services such as children's social care, the local authority designated officer (LADO), the DBS and the police when managing referrals. As well as working closely with the principal.

Our Deputy Designated Safeguarding Lead is Mrs. Eve Strike. Her role is to provide support to the Lead and be available if the Lead is unavailable.

Our Chair of Trustees is Mr. Michael Spooner. His role in Safeguarding is to take the lead in dealing with allegations of abuse made against the Head Teacher.

Our Head Teacher is Mrs. Johanna Esterhuizen. Her role in Safer Recruitment is to ensure that the school operates safe recruitment procedures and makes sure that all appropriate checks are carried out on staff and volunteers who work with the children.

All staff members in the school must read the content of the policy. The *Teacher Standards 2012* states that teachers, including head teachers, should safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties.

All staff must undertake a regular course on safeguarding and child protection that must be updated regularly. The School is committed to an on-going training programme on such matters. Yearly updates will be undertaken at the beginning of each school year.

All staff must staff read Part 1 and Appendix A "Further Information", of Keeping Children Safe in Education (2016). The school has systems in place to assist staff understand and discharge their role and responsibilities". All staff are required to read and sign to indicate they understand the School's safeguarding policies.

The Governors and Trustees recognise the need to build constructive links with childcare agencies, and will work with social care, the police, health services and other services to promote the welfare of children and protect them from harm. Accordingly, these guidelines have been prepared in consultation with the PCCA's Churches Protection Advisory Service, (CCPAS) and Christian Education Europe.

The Governors and Trustees are committed to:

- Listening to, relating effectively and valuing children and young people whilst ensuring their protection within school activities.
- Ensuring safeguarding is taught 'as part of providing a broad and balanced curriculum'
- Employing the expertise of the staff when reviewing safeguarding policies and providing opportunities for staff to contribute to and shape safeguarding arrangements and the child protection policy.
- Encouraging and supporting parents/carers
- Ensuring that staff members are given support and training
- Having a system for dealing with concerns about possible abuse
- Maintaining good links with the statutory child care authorities

Where a child is suffering significant harm, or is likely to do so, action will be taken to protect that child. Action will also be taken to promote the welfare of a child in need of additional support, even if they are not suffering harm or are at immediate risk.

Everyone who encounters children and their families has a role to play in safeguarding children. Anyone working in the school is particularly important as they are in a position to identify concerns early and provide help for children, to prevent concerns from escalating; they form part of the wider safeguarding system for children. For a description of this system, see *Working Together to Safeguard Children 2015*.

All staff members have a responsibility to provide a safe environment in which children can learn. They have a responsibility to identify children who may be in need of extra help or who are suffering, vulnerable, or are likely to suffer, significant harm. Staff have a responsibility to review and monitor the list of these students on a regular basis All staff members then have a responsibility to take appropriate action, working with other services as needed, including Early Help.

Early Help is used to describe the process of taking action early and as soon as possible to tackle problems emerging for children, young people and their families. Effective help can occur at any point in a child or young person's life. Staff should be able to identify the vulnerable children in the school who need who need this level of support. These children should be identified and monitored. Staff need to understand the difference between a safeguarding concern and a child in immediate danger or at significant risk of harm, as part of identifying vulnerable learners.

In addition to working with the designated safeguarding lead staff, staff members should be aware that they might be asked to support social workers to take decisions about individual children.

All staff members should make themselves aware of the systems within the school that support safeguarding, which are explained in the staff induction. This includes the school's safeguarding and child protection policy; the staff code of conduct; and the designated safeguarding lead.

Staff members should be aware of the signs of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection. Knowing what to look for is vital to the

early identification of abuse and neglect. If staff members are unsure they should always speak to children's social care.

Staff members should be aware of any signs of extremist views of any kind in our school, whether from internal sources –students, staff or governors & trustees, or external sources - school community, external agencies or individuals. Our students see our school as a safe place where they can explore controversial issues safely and where our teachers encourage and facilitate this – we have a duty to ensure this happens.

Staff members are advised to maintain an attitude of 'it could happen here' where safeguarding is concerned. When concerned about the welfare of a child, staff members should always act in the interests of the child.

A child going missing from an education setting is a potential indicator of abuse or neglect. Staff members should follow the school's procedures for dealing with children who go missing, particularly on repeat occasions. They should act to identify any risk of abuse and neglect, including sexual abuse or exploitation. More information can be found in this policy about children who run away or go missing from home or care.

If staff members have concerns about a child they should raise these with the school's designated safeguarding lead. This also includes situations of abuse that may involve staff members. The safeguarding lead will usually decide whether to make a referral to children's social care, although any staff member can refer their concerns to children's social care directly. Where a child and family would benefit from co-ordinated support from more than one agency (for example education, health, housing, police) an inter-agency assessment will be conducted. These assessments, undertaken by a lead professional (a teacher, special educational needs co-ordinator, General Practitioner (GP), family support worker, and/or health visitor), will identify what help the child and family require to prevent needs escalating to a point where intervention would be needed via a statutory assessment under the Children Act 1989.

A concern is when you are troubled about a child's welfare and you have reasonable cause to suspect a child is suffering, or likely to suffer, significant harm. It involves the child's safety and well-being.

If, at any point, there is a risk of immediate serious harm to a child a referral should be made to children's social care immediately. Anybody can make a referral. If the child's situation does not appear to be improving, the staff member with concerns should press for re-consideration. Concerns should always lead to help for the child at some point.

It is important for children to receive the right help at the right time to address risks and prevent issues escalating. Research and Serious Case Reviews have repeatedly shown the dangers of failing to take effective action. Poor practice includes: failing to act on and refer the early signs of abuse and neglect, poor record keeping, failing to listen to the views of the child, failing to re-assess concerns when situations do not improve, sharing information too slowly and a lack of challenge to those who appear not to be taking action.

IMPORTANT CONTACT DETAILS:

Safeguarding incidents could happen anywhere and staff should be alert to possible concerns being raised in this school

Safeguarding concerns about adults in the school should be made to the Designated Safeguarding Lead or to the Head Teacher.

Safeguarding concerns about independent school proprietors should go straight to the local authority Designated Officer - the LADO.

To contact the following staff members please call the school office in the first instance:
Contact Number; 0118 988 6464

Mrs J Esterhuizen - the Designated Safeguarding Lead Person for Child Protection
Mrs Eve Strike - the Designated Deputy Lead Person for Child Protection
Mr. Michael Spooner – The Chair of the Trustees
Mr. Michael Spooner - The Chair of Trustees and Safer Recruitment Officer

All staff members may raise concerns directly with Children's Social Care services

To make a Safeguarding/Child Protection Referral contact either:

- The NSPCC Helpline: 0808 800 5000
- The NSPCC whistle-blowing helpline: 0800 028 0285
- The Police: 101 to report crime and other concerns that do not require an emergency response; 999 when there is danger to life or when violence is being used or threatened
- CCPAS: (Lo-call): 0845 120 45 50 or (STD): 01322 517817
- Alternatively contact the local **Wokingham Safeguarding Children Board (WSCB)** on **0118 9746105** or email **WSCB@wokingham.gov.uk** and give as much information as you can.

The school will work with the Local Authority Designated Officer (LADO) as deemed appropriate. The LADO provide advice and guidance to employers and voluntary organisations that have concerns about a person working or volunteering with children and young people who may have behaved inappropriately or you have received information that may constitute an allegation.

CHILD PROTECTION POLICY

The Governors and Trustees recognise that many children and young people today are the victims of neglect, and physical, sexual and emotional abuse, including extremism and radicalisation. Accordingly, the Governors and Trustees have adopted the policy contained in this document, (hereafter "the policy"). The policy sets out agreed guidelines relating to the following areas:

- The Prevent Duty
- Definitions of abuse
- Responding to allegations of abuse, including those made against teachers in the school.
- Appointing teachers/assistants
- Supervision of activities and practice issues
- Helping victims of abuse
- Working with offenders
- Safer Recruitment including the level of DBS checks that will be undertaken for volunteers and Trustees

THE PREVENT DUTY

From Wednesday 1 July 2015, all schools and childcare providers must have due regard to the need to prevent people being drawn into terrorism.

The Governmental definition of extremism is:
'Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs; and/or calls for the death of members of our armed forces, whether in this country or overseas'.

Schools and EYFS providers have a critical part to play. In England, the Early Years Foundation Stage (EYFS) accordingly places clear duties on providers to keep children safe and promote their welfare. To protect children in our care, we must be alert to any safeguarding and child protection issues in the child's life at home or elsewhere.

As a school and EYFS provider, we are expected to demonstrate activity in the following areas:

- Assessing the risk of children being drawn into terrorism.
- Demonstrate that they are protecting children and young people from being drawn into terrorism by having robust safeguarding policies.
- Ensure that their safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children Board.
- Make sure that staff have training that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism
- Expected to ensure children are safe from terrorist and extremist material when accessing the internet

The school holds a separate Preventing Extremism and Radicalisation Policy with regard to this.

The full Government Prevent Strategy can be viewed at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

The full Government Prevent Duty (2015) can be viewed at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

SIGNIFICANT HARM

Some children are in need because they are suffering or likely to suffer significant harm. The Children Act 1989 introduced the concept of significant harm as the threshold that justifies compulsory intervention in family life in the best interests of children. Decisions about significant harm should be informed by a careful assessment of the child's circumstances and discussion between statutory agencies and with the child and family.

DEFINITIONS OF ABUSE

The following definitions of child abuse are taken from the document *'Keeping Children Safe in Education' (2016)*:

Abuse

A form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others (e.g. via the internet). They may be abused by an adult or adults or another child or children.

Physical Abuse

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

Emotional abuse

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

Sexual Abuse

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

Neglect

The persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to: provide adequate food, clothing and shelter (including exclusion from home or abandonment); protect a child from physical and emotional harm or danger; ensure adequate supervision (including the use of inadequate care-givers); or ensure access to appropriate medical care or treatment. It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

SPECIFIC SAFEGUARDING ISSUES

Learners with SEN and Disabilities

Learners with SEN and disabilities have additional safeguarding vulnerabilities:

- Disabled children are at significantly greater risk of physical, sexual and emotional abuse and neglect than non-disabled children
- Disabled children at greatest risk of abuse are those with behaviour/conduct disorders. Other high-risk groups include children with learning difficulties/disabilities, children with speech and language difficulties, children with health-related conditions and deaf children.
- Disabled children are more likely to be abused by someone in their family compared to non-disabled children. The majority of disabled children are abused by someone who is known to them.
- Bullying is a feature in the lives of many disabled children
- Disabled children are more likely to experience the negative aspects of social networking sites than non-disabled children
- Disabled children (and severely disabled children even more so) may disclose less frequently and delay disclosure more often compared to typically developing children. Disabled children are most likely to turn to a trusted adult they know well for help such as family, friend or teacher

Disabled children are at greater risk of abuse and significant barriers can exist to their safeguarding and wellbeing. Understanding a child's needs, building on their strengths, overcoming the barriers and developing innovative solutions for meeting the challenges will not only enhance the child's wellbeing and protection from abuse but will provide learning that may also be of benefit for non-disabled children. Disabled children have an equal right to protection from abuse.

Child Missing from Education

A child going missing from education is a potential indicator of abuse or neglect. School staff should follow the school's procedures for dealing with children that go missing from education, particularly on repeat occasions, to help identify the risk of abuse and neglect, including sexual exploitation, and to help prevent the risks of their going missing in future.

The school has a ***Child Missing from Education*** policy, which we will abide by concerning this area. The school has a ***Child Missing from Education*** policy, written in accordance with the *Children Missing Education Statutory Guidance for Local Authorities - September 2016, which* we will abide by concerning this area.

The school has in place appropriate safeguarding policies, procedures and responses for children who go missing from education, particularly on repeat occasions.

Child Sexual Exploitation

Child sexual exploitation (CSE) is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology.

Child sexual exploitation (CSE) involves exploitative situations, contexts and relationships where young people receive something (for example food, accommodation, drugs, alcohol, gifts, money or in some cases simply affection) as a result of engaging in sexual activities. Sexual exploitation can take many forms ranging from the seemingly 'consensual' relationship where sex is exchanged for affection or gifts, to serious organised crime by gangs and groups. What marks out exploitation is an imbalance of power in the relationship. The perpetrator always holds some kind of power over the victim, which increases as the exploitative relationship, develops. Sexual exploitation involves varying degrees of coercion, intimidation or enticement, including unwanted pressure from peers to have sex, sexual bullying including cyberbullying and grooming. However, it also important to recognise that some young people who are being sexually exploited do not exhibit any external signs of this abuse.

The school holds the following document on file if ever the need arises for such information: "Child Sexual Exploitation Definition and Guide Feb 2017"

Peer-on-Peer Abuse

Peer-on-peer abuse:

- features physical, emotional, sexual and financial abuse of young people by their peers,
- can impact any young person, although the characteristics/experiences of some can be exploited by their peers, or missed by services, making them more vulnerable to abuse than others
- is influenced by the nature of the environments in which young people spend their time
- hinges upon young people's experiences of power, and ultimately the notion of consent
- concepts of abuse are built upon notions of 'power' and therefore 'consent', not to be confused with the age of consent to sexual activity:

    - young people over the age of consent (16 and 17 year olds) can be abused by their peers
    - Many young people who abuse their peers are themselves below the age of consent
- abuse is abuse and should never be tolerated or passed off as "banter" or "part of growing up"

The school will minimise the likelihood of this happening by fully implementing its Behaviour Policy, Anti-Bullying Policy and all other relevant policies.

The school will use resources on such issues to address these matters in PSHE.

Resources on peer-on-peer pressure can be found at:
http://www.msunderstood.org.uk/assets/templates/msunderstood/style/documents/MSUPB01.pdf

Organised Abuse

Organised abuse is sexual abuse where there is more than a single abuser and the adults concerned appear to act in concert to abuse children and/or where an adult uses an institutional framework or position of authority to recruit children for sexual abuse.

Female Genital Mutilation

Female Genital Mutilation (FGM) comprises all procedures involving partial or total removal of the external female genitalia or other injury to the female genital organs. It is illegal in the UK and a form of child abuse with long-lasting harmful consequences.
Staff must personally report to the police a disclosure that FGM has been carried out (in addition to liaising with the DSL.

The school can access the following document if ever the need arises for such information: 'Multi-Agency Statutory Guidance on Female Genital Mutilation' (CEE MOD) or
https://www.gov.uk/government/publications/multi-agency-statutory-guidance-on-female-genital-mutilation

The London Safeguarding Children Board's information on 'Safeguarding Children at Risk of Abuse through Female Genital Mutilation' will also be taken into account:
http://www.londoncp.co.uk/chapters/sg_ch_risk_fgm.html

Honour-Based Violence

So-called Honour Based Violence (HBV) is a term used to describe violence committed within the context of the extended family which are motivated by a perceived need to restore standing within the community, which is presumed to have been lost through the behaviour of the victim. Most victims of HBV are women or girls, although men may also be at risk.

Women and girls may lose honour through expressions of autonomy, particularly if this autonomy occurs within the area of sexuality. Men may be targeted either by the family of a woman who they are believed to have 'dishonoured', in which case both parties may be at risk, or by their own family if they are believed to be homosexual.

Some common triggers for HBV include:

- Refusing an arranged marriage
- Having a relationship outside the approved group
- Loss of virginity
- Pregnancy
- Spending time without the supervision of a family member
- Reporting domestic violence

Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism11. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability, which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media in particular has become a major factor in the radicalisation of young people.

As with managing other safeguarding risks, staff should be alert to changes in children's behaviour, which could indicate that they may be in need of help or protection. School staff should use their professional judgement in identifying children who might be at risk of radicalisation and act proportionately which may include making a referral to the Channel programme.

Honour-based violence

'Honour-based violence' is intended to 'protect or defend family honour' by preventing and punishing a person's violations of family or community 'norms'. A child who is at risk of honour based violence is at significant risk of physical harm (including being murdered) and/or neglect, and may also suffer significant emotional harm through the threat of violence or witnessing violence directed towards a sibling or other family member.

According to the Metropolitan Police Service, an honour-based crime might be committed against someone who:

- becomes involved with a boyfriend or girlfriend from a different culture or religion;
- wants to get out of an arranged marriage;
- wants to get out of a forced marriage;
- Wears clothes or takes part in activities that might not be considered traditional within a particular culture.

The perceived immoral behaviour which could precipitate a murder includes:

- Inappropriate make-up or dress;
- The existence of a boyfriend;
- Kissing or intimacy in a public place;

- Pregnancy outside of marriage;
- Being a victim of rape;
- Inter-faith relationships.

Children sometimes truant from school to obtain relief from being policed at home by relatives. They can feel isolated from their family and social networks and become depressed, which can on some occasions lead to self-harm or suicide.

Families may feel shame long after the incident that brought about dishonour occurred, and therefore the risk of harm to a child can persist. This means that the young person's new boy/girlfriend, baby (if pregnancy caused the family to feel 'shame'), associates or siblings may be at risk of harm.

OTHER SAFEGUARDING ISSUES

Staff need to be aware of the following specific issues. The school holds policies on those marked with an *

Guidance and practical support on these specific safeguarding issues will be sought form expert and professional organisations, if and when needed, using the NSPCC and GOV.UK websites:

• bullying including cyberbullying - see Appendix 3 for our ‘E-Safety Policy’*

• domestic violence

• drugs*

• fabricated or induced illness

• faith abuse

• forced marriage

• gangs and youth violence

• gender-based violence/violence against women and girls (VAWG)

• mental health

• private fostering

• sexting – see Appendix 2 for our ‘Youth-Produced Sexual Imagery Policy’

• teenage relationship abuse

• trafficking

- hate – see our Anti-Bullying Policy Appendix I'

The following has been written using information supplied by The Churches Child Protection Advisory service

RECOGNISING AND RESPONDING TO ABUSE

The following signs may or may not be indications that abuse has taken place, but the possibility should be considered.

Physical Signs of Abuse

- Any injuries not consistent with the explanation given for them.
- Injuries that occur to the body in places that are not normally exposed to falls, rough games, etc.
- Injuries which have not received medical attention
- Neglect – under nourishment, failure to grow, constant hunger, stealing or gorging food, untreated illnesses, inadequate care, etc
- Reluctance to change for, or participate in games or swimming
- Repeated urinary infections or unexplained tummy pains
- Bruises, bites, burns, fractures etc which do not have an accidental explanation
- Cuts/ scratches/ substance abuse

Indicators of Possible Sexual Abuse

- Any allegations made by a child concerning sexual abuse
- Any allegations made by a child concerning female genital mutation
- Child with excessive preoccupation with sexual matters and detailed knowledge of adult sexual behaviour, or who regularly engages in age-inappropriate sexual play
- Sexual activity through words, play or drawing
- Child who is sexually provocative or seductive with adults
- Inappropriate bed-sharing arrangements at home
- Severe sleep disturbances with fears, phobias, vivid dreams or nightmares, sometimes with overt or veiled sexual connotations
- Eating disorders – anorexia, bulimia

Emotional Signs of Abuse

- Changes or regression in mood or behaviour, particularly where a child withdraws or becomes clinging. Also depression/ aggression, extreme anxiety
- Nervousness, frozen watchfulness
- Obsessions or phobias
- Sudden under-achievement or lack of concentration
- Inappropriate relationships with peers and/ or adults
- Attention-seeking behaviour
- Persistent tiredness
- Running away/ stealing/ lying

WHAT TO DO IF YOU SUSPECT THAT ABUSE MAY HAVE OCCURRED

1. You must report concerns as soon as possible to Mrs. J. Esterhuizen (hereafter the "Co-ordinator"), who is nominated by the Governors and Trustees to act on their behalf in referring allegations or suspicions of neglect or abuse to the statutory authorities. She may also be required by conditions of the School Insurance Policy to immediately inform the Insurance Company. In the absence of the Co-ordinator, the matter should be brought to the attention of Mrs. Eve Strike (hereafter the "Deputy Co-ordinator"). In all instances telephone; 0118 988 6464

   If the suspicions in any way involve the Co-ordinator then the report should be made to the Deputy Co-ordinator at the school. If the suspicions in any way implicate both the Co-ordinator and the Deputy Co-ordinator, then the report should be made in the first instance to PCCA Churches' Child Protection Advisory Service (hereafter "CCPAS"), PO Box 133, Swanley, Kent, BR8 7UQ. Telephone 01322 660011 or 01322 667207. Alternatively contact the local Children, Schools and Families department.

2. Suspicions will not be discussed with anyone other than those nominated above.

3. It is, of course, the right of any individual as a citizen to make direct referrals to the child protection agencies or seek advice from CCPAS, although we hope that members of the school will use this procedure. If, however, you feel that the Co-ordinator or Deputy Co-ordinator have not responded appropriately to your concerns, then it is open to you to contact the relevant organisation direct. We hope that by making this statement that we demonstrate the commitment of the school to effective child protection.

ALLEGATIONS OF PHYSICAL INJURY OR NEGLECT

If a child has a physical injury or symptom of neglect, the Co-ordinator will:

1 Contact CCPAS for advice in cases of deliberate injury or where concerned about the child's safety. The school in these circumstances should not inform the parents.
2 Where emergency medical attention is necessary it will be sought immediately. The Co-ordinator will inform the doctor of any suspicions of abuse.
3 In other circumstances speak with the parent/ carer and suggest that medical help/ attention be sought for the child. The doctor (or health visitor) will then initiate further action, if necessary.
4 If appropriate, the parent/ carer will be encouraged to seek help from the CCPAS.
5 Where the parent/ carer is unwilling to seek help, if appropriate, the Co-ordinator will offer to go with them. If they still fail to act, the Co-ordinator should, in cases of real concern, contact CCPAS for advice. CCPAS will confirm its advice in writing in case this is needed for reference purposes in the future.

ALLEGATIONS OF SEXUAL ABUSE

In the event of allegations or suspicions of sexual abuse, the Co-ordinator will:

1 Contact the Police Child Protection Team directly. The Co-ordinator will NOT speak to the parent (or anyone else).
2 If, for any reason, the Co-ordinator is unsure whether or not to follow the above, then advice from CCPAS will be sought and followed. CCPAS will confirm its advice in writing in case this is needed for reference purposes in the future.

3 Under no circumstances will the Co-ordinator attempt to carry out any investigation into the allegation or suspicions of sexual abuse. The role of the Co-ordinator is to collect and clarify the precise details of the allegation or suspicion and to provide this information to the Children, Schools and Families department, whose task it is to investigate the matter under Section 47 of the Children Act 1989.

4 Whilst allegations or suspicions of sexual abuse will normally be reported to the Co-ordinator, the absence of the Coordinator or Deputy should not delay referral to the Children, Schools and Families department.

5 Exceptionally, should there be any disagreement between the person in receipt of the allegation or suspicion and the Co-ordinator or Deputy as to the appropriateness of a referral to the Children, Schools and Families department, that person retains a responsibility as a member of the public to report serious matters to the Children, Schools and Families department, and should do so without hesitation

6 The Governors and Trustees will support the Co-ordinator or Deputy in their role, and accept that any information they may have in their possession will be shared in a strictly limited way on a need to know basis.

HOW TO RESPOND TO A CHILD WANTING TO TALK ABOUT ABUSE

It is not easy to give precise guidance, but the following may help:

General Points

- Show acceptance of what the child says (however unlikely the story may sound)
- Keep calm
- Look at the child directly
- Be honest
- Tell the child you will need to let someone else know – don't promise confidentiality
- Even when a child has broken a rule, they are not to blame for the abuse
- Be aware that the child may have been threatened or bribed not to tell
- Never push for information. If the child decides not to tell you after all, then accept that and let them know that you are always ready to listen

Helpful things you may say or show

- "I believe you"
- Show acceptance of what the child says
- "Thank you for telling me"
- "It's not your fault"
- "I will help you"

Do not say

- "Why didn't you tell anyone before"
- "I can't believe it!"
- "Are you sure this is true?"
- "Why? How? When? Who? Where?"
- Never make false promises
- Never make statements such as " I am shocked, don't tell anyone else"

Concluding

- Again reassure the child what you are going to do next and that you will let them know what happens (you might have to consider referring to the Children, Schools and Families department or the Police to prevent a child or young person returning home if you consider them to be seriously at risk of further abuse)
- Contact the person in the school responsible for coordinating child protection concerns or contact CCPAS for advice or go directly to the Children, Schools and Families department / Police/ NSPCC
- Consider your own feelings and seek pastoral support if needed

WHAT TO DO ONCE A CHILD HAS TALKED TO YOU ABOUT ABUSE

The Procedure

- Make notes as soon as possible (preferably within one hour of the child talking to you), writing down exactly what the child said and when she/he said it, what you said in reply and what was happening immediately beforehand (e.g. a description of the activity). Record dates and times of these events and when you made the record. Keep all hand written notes, even if subsequently typed. Such records should be kept safely for an indefinite period.
  Use the form "Responding to abuse – worker's action sheet"
- Report your discussion as soon as possible to the Co-ordinator. If the latter is implicated report to the Deputy Co-ordinator. If all are implicated, report to CCPAS or to Children, Schools and Families if preferred.
- You should not discuss your suspicions or allegations with anyone other than those nominated in the above point.
- Once a child has talked about abuse the worker/ co-ordinator should consider whether or not it is safe for a child to return home to a potentially abusive situation. On rare occasions, it might be necessary to take immediate action to contact Children, Schools and Families and/ or Police to discuss putting into effect safety measures for the child so that they do not return home.

WORKING WITH OFFENDERS

The Governors and Trustees in their commitment to the protection of all children will meet with the individual and discuss boundaries that the person will be expected to keep.

Offenders will be expected to sign a contract stipulating boundaries and will involve the person's family and partner who will need to be informed.

HELPING VICTIMS OF ABUSE

As a Christian school, we are committed to supporting victims of abuse, and encouraging them in their faith.

The school will ensure the child's wishes or feelings are taken into account when determining what action to take and what services to provide to protect individual children through ensuring there are systems in place for children to express their views and give feedback. Staff members should not promise confidentiality to the child and always act in the interests of the child.

ARRANGEMENTS FOR SUPERVISION OF GROUP/ CHILDREN'S ACTIVITIES

Practical Issues

- A register of children or young people attending the activity should be kept, and a register of helpers.
- A log of each activity, recording any unusual events with each teacher/assistant recording what they witnessed should be kept.
- Incidents such as fights and what action the teacher/assistant took should be recorded in the logbook.
- Accidents and injuries should be recorded in a separate accident book and parents and older children should be asked to sign this.
- No person under 16 years of age should be left in charge of any children of any age. Nor should children or young people attending school be left alone at any time.

Boundaries

- All staff members should treat all children/young people with dignity and respect in attitude, language used and actions.
- Respect the privacy of children, avoid questionable activity.
- If you invite a child to your home, ensure this is with the knowledge of the Head Teacher and that a parent is aware.
- Ensure that all transport arrangements have parental approval and are with the knowledge of the leadership.
- Only staff members assigned to a group should be allowed into rooms. Other adults should not have free access. Ensure you note anybody else who is there for a specific reason in the logbook.

OFF-SITE VISITS/

Appropriate risk assessments must be in place prior to any off-site visit taking place.

Any overnight visit will explicitly set out sleeping arrangements; the role and responsibility of each adult, whether employed or volunteers; on/off duty arrangements; clear expectations about boundaries and interactions with children/young people; and expectations around smoking/drinking by adult.

Safeguarding concerns or allegations will be responded to following the school safe-guarding procedures. The member of staff in charge of the visit will report any safeguarding concerns to the Designated Safeguarding Lead and Head teacher, who will pass to Social Care if appropriate. In an emergency, the staff member in charge will contact the police and/or social care.

POLICY ON SUSPICIONS OR ALLEGATIONS OF CHILD ABUSE INVOLVING SCHOOL STAFF

Staff must be aware that they may be vulnerable to accusations of abuse and must, therefore, be sensitive to a child's reaction to physical contact and react appropriately. During their daily contact with the children, all staff must be aware of the following:

- It is the policy of The Vine Christian School not to kiss the pupils.

- Staff should not touch a child in such a way or on parts of the body that might be considered indecent.
- Staff should avoid restraining children, except under certain circumstances when it is unavoidable (See Policy on Restraint).
- Staff should maintain professional standards of behaviour and appropriate boundaries at all times in relationships between themselves and the pupils, themselves and the parents.
- A member of staff, who feels that they may be at risk of being accused of behaving inappropriately, should request the presence of another member of staff.
- No form of corporal punishment should ever be used nor its use ever threatened.
- When it is necessary to restrain a child to prevent injury to themselves, others or property, only the minimum force should be used and injury to the child concerned should be avoided. Any arm or hands should never be placed around a child's neck.

If there is an allegation or suspicion of misconduct about a member of staff, the Head Teacher must be informed immediately. Failure to do so would result in disciplinary action

If the allegation or suspicion in any way involve the Co-ordinator then the report should be made to the Deputy Co-ordinator, 0118 988 6464. If the suspicions in any way implicate both the Co-ordinator and the Deputy Co-ordinator, then the report should be made in the first instance to PCCA Churches' Child Protection Advisory Service (hereafter "CCPAS"), PO Box 133, Swanley, Kent, BR8 7UQ, 01322 660011 or 01322 667207.

Alternatively contact the local **Wokingham Safeguarding Children Board (WSCB)** on **0118 9746105** or email **WSCB@wokingham.gov.uk** and give as much information as you can.

Since January 2009, the school is required to inform the Independent Safeguarding Agency (ISA) within one month of leaving the school, any person, whether employed, contracted, a volunteer or a student, whose services are no longer used because he or she is considered unsuitable to work with children.

The address for referrals is PO Box 181, Darlington DL1 9FA - Telephone 01325 953743. Failure by the school to make such a report would constitute an offence, leading to the school being removed from the DfE's register of Independent Schools (legislation from The Education (Provision of Information by Independent Schools) (England) Regulations 2003. Compromise Agreements cannot apply in this connection.

The school will also make a referral to the Disclosure and Barring Service (DBS) if a person in regulated activity has been dismissed or removed due to safeguarding concerns, or would have been had they not resigned. This is a legal duty of the school.

Regard must be given to the section 'Allegations of Abuse Made Against Teachers and Other Staff', in the document ''Keeping Children Safe in Education' (2016)', which is on file in the school office.

ALLEGATIONS AGAINST PUPILS

The School's policies on behaviour, bullying, discipline and sanctions should be read in conjunction with this policy and will also apply to this situation. Bullying should be treated as a child protection concern when there is reasonable cause to suspect that a child is suffering or likely to suffer significant harm. A pupil against whom an allegation of abuse has been made may

be suspended from the School during the investigation if it is considered to be in the interests of a child who might otherwise be at risk, in the interests of the pupils at large or to allow the investigation to proceed more effectively.

POLICY ON RESPONSIBILITIES AND ACTIONS TO BE TAKEN IF THE WHEREABOUTS OF A CHILD IS UNKNOWN/ CHILDREN MISSING FROM EDUCATION

In the case of a child being withdrawn from the school and their whereabouts being unknown, the school will endeavour in the first place to make contact with the parents or guardians.

If no communication is received within a week, the school will contact the LEA to enquire whether they have any information regarding the child. If the LEA do not have any facts about the whereabouts of the child we will consult with the LEA about the next step which may involve handing the case over to the local Children's Services.

If this is the case, a note will be made in the Admissions Register stating that the child's whereabouts is unknown and that they have been referred to the LEA. This will be updated if any relevant information is received.

POLICY FOR CHILDREN LOOKED AFTER

The school recognises that children looked after/ children in care are one of the most vulnerable groups of children so need more frequent observational assessment to meet their needs. All staff will be made aware of anyone in the school who is looked after so that the child can be supported adequately. On admission, it will be established who has parental responsibility so that statutory requirements are met.

The school holds a policy for Children Looked After on file.

PHOTOGRAPHY AND IMAGES

To protect children we will:

- Seek parental consent for photographs to be taken or published (for example, on our website or in newspapers or publications)
- Only use school equipment
- Only take photos and videos of children to celebrate achievement
- Use only the child's first name with an image
- Ensure that children are appropriately dressed
- Encourage children to tell us if they are worried about any photographs that are taken of them.

The school will issue a statement that where parents are taking photographs of children related to school events these are to be for personal use only (these are not to be shared on social media for example).

SAFER RECRUITMENT POLICY

APPOINTMENT OF WORKERS

In appointing workers, the following criteria will need to be met:

1 All prospective workers will be asked to complete an application form.

2 The procedure for the appointment will be:
* Completion of application form
* An interview to make sure any past issues are resolved.
* Undertaking all necessary checks as detailed below
* Discussing with the applicant in detail the school's policy on safeguarding children's welfare and expectations in relation to practice issues e.g. supervision of children's activities and workers etc.
* Attaching the new appointee to a more experienced worker for a period of time
* During and at the end of this probationary period, receiving feedback from other workers on the progress of the trainee
* Only then confirming the appointment – perhaps with regular reviews and support where there are particular concerns.

3. The school will verify a candidate's identity, preferably from current photographic ID and proof of address except where, for exceptional reasons, none is available

4. Enhanced DBS checks will be undertaken for all staff, including volunteers who are carrying out relevant, unsupervised activities with the students, and all Governors and Trustees.

5. Those in regulated activity will need an enhanced DBS certificate with barred list check

6. A separate barred list check (List 99 check) will be obtained if an individual will start work in regulated activity before the DBS certificate is available

7. A Prohibition from Teaching Check must be completed for *everyone* engaged in 'teaching work', whether a qualified teacher or not; and recorded on the Single Central Record, to ensure they are not prohibited from teaching, using **Teacher Services** (https://www.gov.uk/guidance/teacher-status-checks-information-for-employers).
Teacher Services can be used to find out if potential new staff have any current prohibitions, restrictions or sanctions using the following lists:
- teachers who have failed to successfully complete their induction or probation period
- teachers who are the subject of a suspension or conditional order imposed by the General Teaching Council for England (prior to its abolition)
- teachers and others who are prohibited from teaching in England
- individuals who have been barred from taking part in the management of an Independent school (including academies and free schools)
- teachers sanctioned (since 18 January 2016) in other EEA member states by an EEA member state regulator of the teaching profession

Even people with QTS, MUST have this prohibition check entered into the Single Central Record.

8. All leaders and managers, including trustees/governors are now required to have a **section 128 Management Check –** This will be included on the school's SCR showing that checks have been according to section 128. This will also be done using Teacher Services (as point 7).

9. In the case of a foreign national, the appropriate overseas body from their country will be contacted for a criminal record check or police clearance. Where this proves unobtainable the Embassy of that country will be contacted to request information on any criminal records that person has. If this proves ineffectual then at least two character references will be taken from citizens residing in that country who know the person well, but this should be a final resort. They must declare if they know of any criminal records held, their relationship with the applicant and their professional capacity, if any. All steps taken must be well documented.

10. Ideally, all foreign nationals should obtain a criminal record check or police clearance before applying for a position with the school.

11. The applicant's right to work in the UK will be checked and evidence kept on record.

12. As part of our Safe Guarding Policy employment will not be offered without the applicant supplying evidence of a full employment history, including information on any gaps

13. Applicants will also be asked to supply a declaration of their mental and physical fitness, concerning their suitability to the position applied for. A job applicant can be asked relevant questions about disability and health in order to establish whether they have the physical and mental capacity for the specific role

14. Two references will be requested

15. Professional qualifications, will be verified, as appropriate

16. The criteria for NOT appointing children's workers are:
    * Previous offences against children
    * If the Governors and Trustees have reservations about an individuals behaviour, lifestyle, attitudes and spiritual commitment.
    * If the Governors and Trustees have any reasons to doubt a worker's suitability for the job.

17. Workers will be given a contract on appointment

18. All new staff will be expected to read the school Code of Conduct Policy and all policies concerning Child Protection and Safeguarding as part of their Induction Process.

19. All new staff will need to complete a Basic Awareness Course on Safeguarding and Child Protection, renewable every three years

20. The school will keep this information on all staff members as to whether or not the following checks have been carried out or certificates obtained, and the date on which the checks were completed, in a single central record.

21. The appointment of workers will be reviewed on a regular basis at an annual meeting using Staff Assessment forms.

22. Teachers/assistants will be given opportunities to meet together with the Principal to discuss work programmes and areas of concern including issues relating to discipline

EXTERNAL VISITORS/CONTRIBUTORS/SPEAKERS

Visitors with a professional role, such as the school nurse, social worker, educational psychologist or members of the Police will have had the appropriate vetting checks undertaken by their own organisation. Any professionals visiting the school should provide evidence of their professional role and employment details (an identity badge for example). If felt necessary, the school will contact the relevant organisation to verify the individual's identity.

The school has a separate policy for visiting speakers.

AGENCY STAFF

The school will check that any agency staff member attending the school is the same person that the agency has provided the vetting checks for.

This policy is written in line with our:

- Preventing Extremism and Radicalisation Policy
- Whistleblowing Policy
- E-Safety Policy
- Behaviour Policy
- Anti-bullying Policy
- Missing Children Policy
- Staff Code of Conduct Policy

These are all available on request from the school office.

RENEWAL OF DBS CHECKS

Information taken from: (https://www.teachers.org.uk/sites/default/files2014/ecr31-dbs-checks.doc).

Since there has never been a requirement for a rolling programme of three-yearly checks for staff who have unbroken service, DBS checks will only be renewed if there has been a break of three months or more. However, a return to work after a period of statutory leave (e.g. maternity, adoption, parental leave, sabbatical, or sickness), is not a new appointment, nor a break in service, as long as the employment remains continuous, therefore a DBS check is not required by law.

The only reference to three-year checks in *Safeguarding Children and Safer Recruitment in Education* (the DfE's statutory guidance prior to *'Keeping Children Safe in Education….'*) was at Appendix 11, where it was **recommended** for agency staff only. Such routine checks for staff directly employed by the school are not required and are considered to be excessive, as they go beyond what the law requires or the Government recommends.

If a new staff member has previously been DBS checked, there is no statutory requirement that another DBS check is carried out *before* taking up a job in our school, provided they

have continuous service and the check is at the correct level for the new post, other than a check of the Barred Lists.

In this case the school will carry out a risk assessment to assess whether the check is at the correct level for the current role, whether it is accurate and whether they trust the previous organisation to have carried out the check efficiently.

The school will ask for evidence from the previous school, college, local authority or supply agency, that the check was undertaken.

However, the school will ensure that an enhanced DBS check is undertaken as soon as possible for the school Single Central Records, or use the update service if the employee is subscribed to this service.

SAFETY MATTERS

The school's arrangements to fulfil other safeguarding and welfare responsibilities are as follows:

Ensure high standards of provision and care for children and learners
Actively promote equality and diversity
Tackle bullying and discrimination immediately
Actively promote British values
Prevent radicalisation and extremism
Ensure that all persons know how to complain and understand the process for doing so
Ensure that children and learners are protected and feel safe.
Challenge any discriminatory behaviour and give help and support to children about how to treat others with respect
Consistently promote positive behaviour
Ensure that all children and learners can identify a trusted adult with whom they can communicate about any concerns, and know that these adults will listen to them and take their concerns seriously
Ensure that written records are made in a timely way and held securely where adults working with children or learners are concerned about their safety or welfare. Those records will be shared appropriately and, where necessary, with consent.
Make clear risk assessments
Oversee the safe use of technology by ensuring that our policies and procedures are adhered to Use an Acceptable Use Agreement
Carefully select and vet staff and volunteers working with children and learners according to statutory requirements.
Check all staff using Enhanced DBS checks
Ensure that all staff have regular Child Protection and Safeguarding Training
Ensure that the Designated Safeguarding Leads undertake training at two-yearly intervals, and in addition receive an update at least yearly
Ensure that the Designated Safeguarding Leads have a job description, and clear cover arrangements. DSLs will be drawn from the senior leadership team and will be the persons carrying out the day-to-day work of safeguarding and child protection. Their responsibilities will not be delegated to others. See Appendix 1.
Keep the Single Central Record up to date
Regularly review safeguarding policies and procedures to keep all children and learners safe

Policy Adopted by Governors and Trustees on: _____

Policy Last Reviewed on: _____

Policy Due for Review on: _____

Signed: _____ (Chair)

Appendix 1

ROLE AND RESPONSIBILITIES OF THE SCHOOL DESIGNATED SAFEGUARDING LEAD

The School Designated Safeguarding Lead (DSL) is the first point of contact for any member of the school staff who has a concern about the safety and well-being of a student.

The DSL does not need to be a member of the teaching staff but should be a recognised member of the Senior Management Team with the required status and authority to carry out the requirements of the role.

Depending on the size and requirements of the school a Deputy Designated Safeguarding Lead should be available. The deputy is the first point of contact in the absence of the DSL to avoid any unnecessary delays in responding to a student's needs.

The DSL and Deputy are required to undertake child protection training every two years and should supplement this training by attending workshops where available, at least annually.

Requirements:

• To have the skills and ability to identify signs of abuse.

• To know how to refer concerns to the appropriate investigating agencies.

• Maintain detailed and accurate written records of child protection concerns and ensure they are kept securely.

• Offer support, advice and give a level of expertise to all members of the school staff team.

• Ensure that all staff have access to and understand the school Safeguarding and Child Protection Policy and Procedures.

• To be able to provide basic awareness/child protection training as part of the induction for all new staff in the school and be part of any other relevant training.

• Be responsible with the Head Teacher for the annual review and update of the School Safeguarding Policy and the presentation of this to the Governing Body.

• Ensure that a copy of the School Safeguarding and Child Protection Policy is available for any parents who request to see it.

• Ensure that the Head Teacher and Chair of Trustees are updated on a regular basis about all issues and child protection investigations.

• Ensure that relevant safeguarding files are copied and forwarded appropriately when a child/young person transfers to another school.

• Be part of the team who review and monitor any causes of concern relating to students which are raised in school

Appendix 2

YOUTH-PRODUCED SEXUAL IMAGERY POLICY

Also known as 'Sexting'

This policy is linked to the school's Safeguarding and Child Protection policies.

INTRODUCTION

Youth-produced sexual imagery is imagery that is being created by under 18s themselves and involves 'sexual imaging', still photographs, 'sexting', video, and streaming. Sexual content is different to indecent - indecent is subjective and has no specific definition in UK law. 'Sexual imaging' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However, The Vine Christian school takes a pro-active approach in its ICT and Enrichment programmes to help students to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

There are a number of definitions of 'sexual imaging' and 'sexting' but for the purposes of this policy sexual imaging is simply defined as images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

There are many different types of sexual imaging (see Supplement 2) and it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. However, it is important that The Vine Christian School applies a consistent approach when dealing with an incident to help protect young people and the school, and the response should always be guided by the 'principle of proportionality'. The primary concern at all times should be the welfare and protection of the young people involved. For this reason the Designated Safeguarding Lead (or Headteacher in the absence of the DSL) needs to be informed of any 'sexual imaging' incidents. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All colleagues are expected to be aware of this policy.

The decisions made by the Designated Safeguarding Lead will be guided by a pathway found at: http://www.mscb.org.uk/pdf/Annex%201-Sexual imaging%20FEB13%20(2).pdf

THE LAW

Making, possessing, and distributing any imagery of someone under 18 which is indecent is illegal. This includes imagery of taken by someone of themselves if they are under 18.

Indecent is not definitively defined in law, but images are likely to be considered indecent if they depict:

- a naked young person
- a topless girl
- an image which displays genitals, and
- sex acts including masturbation.

- indecent images may also include overtly sexual images of young people in their underwear

These laws weren't created to criminalise young people but to protect them. Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support, and safeguarding, not criminalisation.

The National Police Chiefs' Council (NPCC) is clear that "youth-produced sexual imagery should be primarily treated as a safeguarding issue."

Schools may respond to incidents without involving the police. (However, in some circumstances, the police must always be involved.) Images may be deleted and incident managed in school by using a risk-based approach.

STEPS TO TAKE IN THE CASE OF AN INCIDENT

STEP 1 - DISCLOSURE BY A STUDENT

Sexual imaging disclosures should follow the normal safeguarding practices and protocols (see Safeguarding Policy).

A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to police or social services; parents should be informed as soon as possible (police advice permitting).

The following questions will help decide upon the best course of action:

- Is the student disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed?
- For this reason a member of the Safeguarding team should be involved as soon as possible.
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device?
- Does the student need immediate support and/or protection?
- Are there other students and/or young people involved?
- Do they know where the image has ended up?

Assessing the risks once the images have been shared

- Has it been shared with the knowledge of the young person?
- Are adults involved in the sharing?
- Was there pressure to make the image?
- What is the impact on those involved?
- Does the child or children have additional vulnerabilities?
- Has the child taken part in producing sexual imagery before?

STEP 2 - SEARCHING A DEVICE – WHAT ARE THE RULES?

Please refer to the school's Search and Confiscation Policy which is based on the most current legislation: The 2011 Education Act.

The policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device the following conditions should apply:

- The action is in accordance with the school's policies regarding Safeguarding and Searching and Confiscation.
- The search is conducted either by the head teacher or a person authorised by them (or Deputy Head or Designated Safeguarding Lead) and one other person
- A member of the safeguarding team should normally be present
- The search should normally be conducted by a member of the same gender as the person being searched. However if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.

If any illegal images of a young person are found the Safeguarding Team will discuss this with the Police (see Appendices 1, 2 and 3).

The Association of Chief Police Officers (ACPO) advise that as a general rule it will almost always be proportionate to refer any incident involving 'aggravated' sharing of images to the Police, whereas purely 'experimental' conduct may proportionately dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

'Experimental conduct' commonly refers to that shared between two individuals (e.g. girlfriend and boyfriend) with no intention to publish the images further (see Supplement 2). Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

If an 'experimental' incident is not referred to the Police, the reasons for this should be recorded in the school's 'Safeguarding Incidents Log'.

Always put the young person first. Do not search the device if this will cause additional stress to the student/person whose image has been distributed. Instead rely on the description by the young person, secure the advice and contact the Police.

Never:

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest not to do so would impede a police inquiry.
- View the image unless it is unavoidable. Instead, respond to what you have been told the image contains.
- Copy, print or share any material for evidence (it is illegal)
- Move any material from one storage device to another
- Discuss with parents, unless there is an issue where that's not possible

Always:

- Refer to the Designated Safeguarding Lead, who is able to take any necessary strategic decisions.
- If it is felt necessary to view the image, discuss with the Head teacher or DSL first, and view with another member of staff present
- Record the fact that the images were viewed along with reasons and who was present. Sign and date.
- Record the incident. The Safeguarding Team employ a systematic approach to the recording of all safeguarding issues
- Act in accordance with school safeguarding search and confiscation policies and procedures
- Contact social care or the police if there is any concern that the young person is at risk of harm

If there is an indecent image of a child on a website or a social networking site then the Safeguarding Team will report the image to the site hosting it. Under normal circumstances the team would follow the reporting procedures on the respective website; however, in the case of a sexual imaging incident involving a child or young person where it may be felt that they may be at risk of abuse then the team will report the incident directly to CEOP: www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

Once the DSL has enough information, the decision should be made whether to deal with the matter in school or refer it to the police/social care. All information and decision-making should be recorded in line with school policy. If the incident has been dealt with in school, a further review should be held to assess risks.

The DSL should always refer to the police or social care if incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent, [e.g., SEN]
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)

STEP 3 - WHAT TO DO AND NOT DO WITH THE IMAGE

If the image has been shared across a personal mobile device:

Always

- Confiscate and secure the device(s). Close down or switch the device off as soon as possible. This may prevent anyone removing evidence 'remotely'.

Never

- View the image unless there is a clear reason to do so or view it without an additional adult present (this additional person does not need to view the image and certainly should not do so if they are of a different gender to the person whose image has been shared). The viewing of an image should only be done to establish that there has been an incident which requires further action.
- Send, share or save the image anywhere (**this is illegal)**
- Allow students to do any of the above

If the image has been shared across a school network, a website or a social network:

Always

- Block the network to all users and isolate the image

Never

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in the school's safeguarding and child protection policies and procedures.

Deleting images (from devices and social media)

If the school decides that involving other agencies is not necessary, consideration should be given to deleting the images.
It is recommended that pupils are asked to delete the images themselves and confirm they have done so. This should be recorded, signed, and dated.
Any refusal to delete the images should be treated seriously, reminding the pupil that possession is unlawful.

STEP 4 - WHO SHOULD DEAL WITH THE INCIDENT?

Often, the first port of call for a student is a class teacher. Regardless of who the initial disclosure is made to she/he must act in accordance with the school safeguarding and/or child protection policy, ensuring that a member of the Safeguarding Team and a senior member of staff are involved in dealing with the incident.

The Designated Safeguarding Lead should always record the incident. The Headteacher should also always be informed- usually by the DSL. There may be instances where the image needs to be viewed and this should be done in accordance with protocols and only if unavoidable.

STEP 5 - DECIDING ON A RESPONSE

There may be many reasons why a student has engaged in sexual imaging – it may be a romantic/sexual exploration scenario or it may be due to coercion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident (see Supplement 1 for definitions). However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

If indecent images of a young person are found:

- Act in accordance with the Safeguarding policy i.e. inform the Safeguarding Team
- Store the device securely
- The Safeguarding Team should carry out a risk assessment in relation to the young person (Use Appendices 2 and 3 for support)
- The Safeguarding Team will make a referral if needed
- The Safeguarding Team will contact the police (if appropriate). Referrals may be made to Social Care but where a crime may thought to have taken place the police are the first port of call. Young persons who have engaged in 'experimental sexual imaging' which is contained between two persons will be referred to Social Care for support and guidance. Those who are felt to be victims of 'sexual imaging' will also be referred to Social Care at a point where the police feel that this will not impede an investigation.
- The young person's Supervisor will put the necessary safeguards in place for the student, e.g. they may need counselling support or immediate protection.
- Inform parents and/or carers about the incident and how it is being managed.

STEP 6 - CONTAINMENT AND PREVENTION

The young persons involved in 'sexual imaging' may be left feeling sensitive and vulnerable for some time. They will require monitoring by and support from their Guidance/Pastoral teams.

Where cases of 'sexual imaging' become widespread or there is thought to be the possibility of contagion then the school will reinforce the need for safer 'online' behaviour using a variety of resources (see http://www.mscb.org.uk/pdf/Annex%201-Sexual imaging%20FEB13%20(2).pdf).

Other staff may need to be informed of incidents and should be prepared to act if the issue is continued or referred to by other students. The school, its students and parents should be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected.

The students' parents should usually be told what has happened so that they can keep a watchful eye over the young person especially when they are online at home.

STEP 7 - REVIEW OUTCOMES AND PROCEDURES WITH THE AIM OF PREVENTING FUTURE INCIDENTS

The frequency or severity of such incidents may be such that the school will need to review its approach. Where this is the case The Vine Christian School will do the following:

- ensure that key policies e.g. Safeguarding, Anti- Bullying, Authorised User Policies are still relevant and can meet emerging issues.
- ensure that the school's infrastructure and technologies are robust enough to meet new challenges.
- ensure that both adults and young persons are alerted to the issues such as safety mechanisms, support mechanisms and the legal implications of such behaviour.
- use the Ofsted framework for Behaviour and Safety as a benchmark to test the strength of the school's approach.

Sexual imaging incidents relate to self-generated images on personally-owned devices, generally outside of school. The Vine Christian School will adopt preventative education strategies for its young people and put in place appropriate staff training to identify and manage incidents. The following are resources currently available:

- CEOP resources at www.thinkuknow.co.uk. There is a film called Exposed and accompanying lesson plans for 11-16 year olds.

- The children's charity Childnet www.childnet-int.org have developed a drama for secondary school-aged children on the issue of sexual imaging.
- Teachtoday is a source of advice for teachers on a variety of topics and does include information on the issue of sexual imaging www.teachtoday.eu.
- The Southwest Grid for Learning have developed a resource for young people: 'So you got naked online' www.swgfl.org.uk/sexual imaging help which supports them in knowing what to do if things have gone wrong online

Appendix 2

YOUTH-PRODUCED SEXUAL IMAGERY POLICY - SUPPLEMENT 1

THE LEGAL POSITION

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken;
- make an indecent photograph (this includes downloading or opening an image that has been sent via email);
- distribute or show such an image;
- possess with the intention of distributing images;
- advertise; and
- possess such images

While any decision to charge individuals for such offences is a matter for the Crown Prosecution Service, it is unlikely to be considered in the public interest to prosecute children. However, children need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and on some occasions media equipment could be removed. This is more likely if they have distributed images.

The decision to criminalise children and young people for sending these kinds of images is a little unclear and may depend on local strategies. However, the current Association of Chief Police
Officers (ACPO) position is that: *'ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.'*

However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a school, we will want to consider the implications of reporting an incident over to the police, it is not our responsibility to make decisions about the seriousness of the matter; that responsibility lies with the Police and the CPS hence the requirement for the school to refer.

In summary sexual imaging is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child.

YOUTH-PRODUCED SEXUAL IMAGERY POLICY - SUPPLEMENT 2

DIFFERENT LEVELS OF SEXUAL IMAGING

The following is adapted from Wolak and Finkelhor *'Sexual imaging: a Typology'.* March 2011

Aggravated incidents involving criminal or abusive elements beyond the creation, sending or possession of youth-produced sexual images

- **Adult offenders** develop relationships with and seduce underage teenagers, in criminal sex offences even without the added element of youth-produced images. Victims may be family friends, relatives, community members or contacted via the Internet. The youth produced sexual images generally, but not always, are solicited by the adult offenders.

- **Youth Only**: **Intent to Harm** cases that:
    - arise from interpersonal conflict such as break-ups and fights among friends
    - involve criminal or abusive conduct such as blackmail, threats or deception
    - involve criminal sexual abuse or exploitation by juvenile offenders.

- **Youth Only: Reckless Misuse** no intent to harm but images are taken or sent without the knowing or willing participation of the young person who is pictured. In these cases, pictures are taken or sent thoughtlessly or recklessly and a victim may have been harmed as a result, but the culpability appears somewhat less than in the malicious episodes.

Experimental incidents involve the creation and sending of youth-produced sexual images, with no adult involvement, no apparent intent to harm or reckless misuse.

- **Romantic episodes** in which young people in ongoing relationships make images for themselves or each other, and images were not intended to be distributed beyond the pair.

- **Sexual Attention Seeking** in which images are made and sent between or among young people who were not known to be romantic partners, or where one youngster takes pictures and sends them to many others or posts them online, presumably to draw sexual attention.

- **Other:** cases that do not appear to have aggravating elements, like adult involvement, malicious motives or reckless misuse, but also do not fit into the Romantic or Attention Seeking sub-types. These involve either young people who take pictures of themselves for themselves (no evidence of any sending or sharing or intent to do so) or pre-adolescent children (age 9 or younger) who did not appear to have sexual motives.

Appendix 3

E-SAFETY AND DATA PROTECTION POLICY

This policy has been written using information from *Herts for Learning* © Herts for Learning

INTRODUCTION

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At The Vine Christian School, we understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to

remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, Trustees & Governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

MONITORING

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

BREACHES

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows:

Mrs J Esterhuizen - the Designated Safeguarding Lead Person for Child Protection
Mrs Eve Strike - the Designated Deputy Lead Person for Child Protection

Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

COMPUTER VIRUSES

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

DATA SECURITY

The accessing and appropriate use of school data is something that the school takes very seriously.

The Local Authority guidance documents listed below

HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Head teacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts

SECURITY

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)
- Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent

PROTECTIVE MARKING OF OFFICIAL INFORMATION

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

RELEVANT RESPONSIBLE PERSONS

Senior members of staff should be familiar with information risks and the school's response.

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

The SIRO in this school is Mr Martin Fuller.

INFORMATION ASSET OWNER (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff should be able to identify across the school:

- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of
-

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several individuals, whose roles involve such responsibility.

However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The IAO in this school is Mr Martin Fuller

Appendix 3

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 1998
  https://ico.org.uk/for-organisations/education/
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- The school's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data* likely to be held on the storage media?
  - How it was disposed of e.g. waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner Website

https://ico.org.uk/

Data Protection Act – data protection guide, including the 8 principles

https://ico.org.uk/for-organisations/education/

EMAIL

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

MANAGING E-MAIL

- The school gives all staff & Trustees & Governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Staff, Trustees & Governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Head teacher

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail

- Staff must inform (the e-Safety coordinator or Head Teacher) if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the Computing Programme of Study

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

SENDING E-MAILS

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section

- *E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED* **INFORMATION**

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- School e-mail is not to be used for personal advertising

RECEIVING E-MAILS

- Check your e-mail regularly

- Activate your ‘out-of-office’ notification when away for extended periods

- Never open attachments from an untrusted source; consult your network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION

Where your conclusion is that e-mail must be used to transmit such data obtain express consent from your Head Teacher to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect.
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

EQUAL OPPORTUNITIES: PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities should be planned and well managed for these children and young people.

E-SAFETY ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the Head Teacher and Trustees & Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Appendix 3

The named e-Safety co-ordinator in this school is Mr. Babu Samuel who has been designated this role as a member of the governors. All members of the school community have been made aware of who holds this post.

It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management, Trustees & Governors are updated by the e-Safety co-ordinator and all Trustees & Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Trustees & Governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

E-SAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in Computing/ICT/ PSHE lessons in the afternoon curriculum plan.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages in the form of training days.

- Details of the ongoing staff training programme can be found in the staff personal files.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see e-Safety Co-ordinator)
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

MANAGING THE SCHOOL E-SAFETY MESSAGES

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The e-Safety policy will be introduced to the pupils at the start of each school year
- E-Safety posters will be prominently displayed
- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities and so on

INCIDENT REPORTING, E-SAFETY & INFRINGEMENTS

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or e-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owner.

E-SAFETY INCIDENT LOG

Some incidents may need to be recorded if they relate to a bullying, extremism or racist incident.

http://www.thegrid.org.uk/eservices/safety/incident.shtml

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints and/ or issues relating to e-Safety should be made to the e-Safety co-ordinator or Head teacher

All incidents should be logged.

INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Head teacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

Flowcharts for Managing an e-Safety Incident may be found at:
http://www.thegrid.org.uk/eservices/safety/incident.shtml

INTERNET ACCESS

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

MANAGING THE INTERNET

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

INTERNET USE

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Head Teacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

INFRASTRUCTURE

- Our school employs some additional web-filtering which is the responsibility of Mr. Martin Fuller who is the school's Network Manager
- IT use is monitored using a pro-active monitoring system.
- However, the school will avoid internet filter 'over-block' as this may place 'unreasonable restrictions on what children can be taught'.
- The Vine Christian School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head Teacher
- If there are any issues related to viruses or anti-virus software, the network manager should be informed by email.

MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies (including social networking sites, if used responsibly both outside and within an educational context) can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online

- Our pupils are asked to report any incidents of Cyberbullying to the school

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

PARENTAL INVOLVEMENT

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

- Parents/carers are expected to sign an acceptable use agreement

- The school disseminates information to parents relating to e-Safety where appropriate in the form of:

    - Information evenings
    - Practical training sessions e.g. current e-Safety issues
    - Posters
    - School website information
    - Newsletter items

PASSWORDS AND PASSWORD SECURITY

PASSWORDS

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform The Head Teacher immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within 2 weeks.

If you think your password may have been compromised or someone else has become aware of your password report this to your Head Teacher

PASSWORD SECURITY

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, learning platform and Management Information System log-in username. Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the school learning platform, virtual

learning environment or other online application to the browser/cache options (shared or private computer)

- In our school, all ICT password policies are the responsibility of Mrs. H Gardner and all staff and pupils are expected to comply with the policies at all times

ZOMBIE ACCOUNTS

'Zombie accounts' refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorised access

PERSONAL OR SENSITIVE INFORMATION

PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared Copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Guidance on How to Encrypt Files can be found on the following site:

http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
Guidance can be found:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Head Teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Head Teacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the ICT Manager or Head Teacher has authority to upload to the internet.

Further information relating to issues associated with school websites and the safe use of images in schools may be found at:

http://www.thegrid.org.uk/schoolweb/safety/index.shtml
http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

STORAGE OF IMAGES

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- Mrs. H Gardner has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

VIDEO CONFERENCING

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Head Teacher is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS (previously CRB) checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Further information and guidance relating to Video Conferencing may be found at:
http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

SCHOOL ICT EQUIPMENT

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You

are responsible for the backup and restoration of any of your data that is not held on the school's network

- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all school ICT equipment to the school. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the Head Teacher.
    - maintaining control of the allocation
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

PORTABLE & MOBILE ICT EQUIPMENT

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus

updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- This technology may be used for educational purposes, as mutually agreed with the Head Teacher. The device user, in this instance, must always ask the prior permission of the bill payer

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

- Never use a hand-held mobile phone whilst driving a vehicle

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

- The school does not provide any mobile devices

TELEPHONE SERVICES

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others

    2. They are not for profit or to premium rate services

    3. They conform to this and other relevant school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask Mrs. M.A. Edwards

REMOVABLE MEDIA

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section ‘

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA’

- Always consider if an alternative solution already exists

- Only use recommended removable media

- Encrypt and password protect

- Store all removable media securely

Removable media must be disposed of securely by your ICT support team

SOCIAL MEDIA

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter to communicate with parents and carers. Mrs. H Gardner is responsible for all postings on these technologies and monitors responses from others

- Staff are not permitted to access their personal social media accounts using school equipment at during from school during school hours

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media

- Pupils are not permitted to access their social media accounts whilst at school

- Staff, Governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, Governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

- Staff, Governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

SERVERS

The Vine Christian School abides by the following criteria:

- Always keep servers in a locked and secure environment

- Limit access rights

- Always password protect and lock the server

- Existing servers should have security software installed appropriate to the machine's specification

- Backup tapes should be encrypted by appropriate software

- Data must be backed up regularly

- Backup tapes/discs must be securely stored in a fireproof container

- Back up media stored off-site must be secure

SYSTEMS AND ACCESS

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

WRITING AND REVIEWING THIS POLICY

STAFF AND PUPIL INVOLVEMENT IN POLICY CREATION

Staff, Governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through staff and governors meetings.

REVIEW PROCEDURE

There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue that concerns them

There will be on-going opportunities for staff to discuss with the AIO any issue of data security that concerns them

This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been read, amended and approved by the staff, head teacher and Governors.

Appendix 3

The Vine Christian School

Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough

The Vine Christian School

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs. H Gardner.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂----------

Parent/ carer signature

We have discussed this document with ……..... (Child's name) and we agree to follow the e-Safety rules and to support the safe use of ICT at The Vine Christian School.

Parent/ Carer Signature ……..…….……

Class …… Date ……

Appendix 3

The Vine Christian School

Senior Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
- I am aware that when I take images of pupils and/ or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day
- I will not sign up to online services until I am old enough to do so

The Vine Christian School

Dear Parent/ Carer

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent/ carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with the Head Teacher

Please return the bottom section of this form which will be kept on record at the school

✂----------

Parent/ carer signature

We have discussed this document with…….. (Child's name) and we agree to follow the e-Safety rules and to support the safe use of ICT at The Vine Christian School.

Parent/ Carer Signature ……..…….……

Pupil Signature……..

Class …… Date ……

Appendix 3

The Vine Christian School

Parent/Carer
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all parents/carers are aware of their parental responsibilities regarding using any form of ICT in relation to the school. All parents are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs. H Gardner

- I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.

- I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.

- I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases).

- I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.

I/we agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……..... (Printed)

Child's Name ……

Relationship to child ……..

Signature …… Date ……

Full Name ……..... (Printed)

Child's Name ……

Relationship to child ……..

The Vine Christian School

Staff, Trustee, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs. H Gardner

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head Teacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head Teacher. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Mrs H Gardner
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Head Teacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm.
-

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..... (Printed)

Job title …….

HELP AND SUPPORT

Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 1998. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on e-Safety - http://www.thegrid.org.uk/eservices/safety/index.shtml

Further guidance - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848

Test your online safety skills http://www.getsafeonline.org

Data Protection Team – email - data.protection@hertfordshire.gov.uk

Information Commissioner's Office – www.ico.org.uk

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015 – this is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision – https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

For additional help, email school.ictsupport@education.gsi.gov.uk

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It

is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

ACTS RELATING TO THE PROTECTION OF PERSONAL DATA

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

COUNTER-TERRORISM AND SECURITY ACT 2015 (PREVENT), ANTI-RADICALISATION & COUNTER-EXTREMISM GUIDANCE

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services