Batford Nursery School,
Harpenden & Rural Children's Centres,
Skylarks Day Care,
Holcroft Road, Harpenden, AL5 5BQ
Telephone: 01582 713872
Headteacher and Head of Centre: Sue Mansfield
www.batfordearlyyearscentre.org.uk
Email: admin@batfordnursery.herts.sch.uk
admin@harpendenandrural.cc
skylarks@batfordnursery.herts.sch.uk

Batford Early Years Centre

Child Protection Policy

Next Review date: March 2018

Signed…… Head of Centre / Headteacher Date: March 2017

Signed…… Chair of Governing Body Date:

To Contact Ofsted: Tel: 0300 123 1231
Email: enguiries@ofsted.gov.uk
Or: www.ofsted.gov.uk

Batford Nursery | Children's Centres | Skylarks Day Care | Batford Nursery | Skylarks Day Care

C O N T E N T S

1	**Introduction**
2	**Statutory Framework**
3	**The Designated Senior Person**
4	**The Governing Body**
5	**When to be concerned**
6	**Dealing with a Disclosure**
7	**Record Keeping**
8	**Confidentiality**
9	**School Procedures**
10	**Communication with parents**
11	**Allegations Involving School Staff/Volunteers**
Appendix 1	**Link to Keeping Children Safe in Education (DfE, 2016)** **Part One: Information for all school staff and Annex A :Further information**
Appendix 2	**Declaration for staff:** **Child Protection Policy and Keeping Children Safe in Education (DfE, 2016)**
Appendix 3	**What to do if you're worried a child is being abused: advice for practitioners flowchart (DfE 2015)**
Appendix 4	**Indicators of abuse and neglect**

1. INTRODUCTION

This policy has been adopted by Batford Early Years Centre which is made up of Batford Nursery School, Skylarks Day Care Limited and the Harpenden and Rural children's Centre Group. Where the word school appears in this document, the reader should understand that this refers to all three departments of Batford Early Years Centre.

Safeguarding is defined as protecting children from maltreatment, preventing impairment of health and/or development, ensuring that children grow up in the provision of safe and effective care and taking action to enable all children to have the best life chances.

This Child Protection Policy forms part of a suite of documents and policies which relate to the safeguarding responsibilities of the school.

In particular this policy should be read in conjunction with the Safer Recruitment Policy, Behaviour Policy, Physical Intervention Policy, Anti-Bullying Policy, Code of Professional Conduct, E-safety Policy.

Purpose of a Child Protection Policy	To inform staff, parents, volunteers and governors about the school's responsibilities for safeguarding children. To enable everyone to have a clear understanding of how these responsibilities should be carried out.
Hertfordshire Safeguarding Children Board Inter-agency Child Protection and Safeguarding Children Procedures	The school follows the procedures established by the Hertfordshire Safeguarding Children Board; a guide to procedure and practice for all agencies in Hertfordshire working with children and their families. **www.hertssafeguarding.org.uk**
School Staff & Volunteers	All school staff have a responsibility to provide a safe environment in which children can learn. School staff and volunteers are particularly well placed to observe outward signs of abuse, changes in behaviour and failure to develop because they have daily contact with children. All school staff will receive appropriate safeguarding children training (which is updated regularly – Hertfordshire Safeguarding Children Board advises every three years), so that they are knowledgeable and aware of their role in the early recognition of the indicators of abuse or neglect and of the appropriate procedures to follow. In addition all staff members should receive safeguarding and child protection updates (for example, via email, e-bulletins and staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

	Temporary staff and volunteers will be made aware of the safeguarding policies and procedures by the Designated Senior Person-including Child Protection Policy and Code of Professional Conduct Establish and maintain an environment where children feel secure, are encouraged to talk, and are listened to when they have a worry or concern.
We Will	Establish and maintain an environment where school staff and volunteers feel safe, are encouraged to talk and are listened to when they have concerns about the safety and well-being of a child. Ensure children know that there are adults in the school whom they can approach if they are worried. Ensure that children, who have additional/unmet needs are supported appropriately. This could include referral to early help services or specialist services if they are a child in need or have been / are at risk of being abused and neglected. Consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. Ensure that staff members working with children 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.
Implementation, Monitoring and Review of the Child Protection Policy	The policy will be reviewed annually by the governing body. It will be implemented through the school's induction and training programme, and as part of day to day practice. Compliance with the policy will be monitored by the Designated Senior Person and through staff performance measures.

2. STATUTORY FRAMEWORK

In order to safeguard and promote the welfare of children, the school will act in accordance with the following legislation and guidance:

- The Children Act 1989
- The Children Act 2004
- Education Act 2002 (Section 175/157)
  Outlines that Local Authorities and School Governing Bodies have a responsibility to " ensure that their functions relating to the conduct of school are exercised with a view to safeguarding and promoting the welfare of children who are its pupils".
- Hertfordshire Safeguarding Children Board Inter-agency Child Protection and Safeguarding Children Procedures (Electronic)
- Keeping Children Safe in Education (DfE, September 2016)
- Keeping Children Safe in Education: Part One- information for all school staff (DfE, September 2016) – APPENDIX 1
- Working Together to Safeguard Children (DfE 2015)
- The Education (Pupil Information) (England) Regulations 2005
- Sexual Offences Act (2003)
- Section 26, The Counter Terrorism and Security Act 2015 (PREVENT duty)
- Female Genital Mutilation Act 2003 (Section 74 ,Serious Crime Act 2015)

Working Together to Safeguard Children (DfE 2015) requires each school to follow the procedures for protecting children from abuse which are established by the Hertfordshire Safeguarding Children Board.

Schools are also expected to ensure that they have appropriate procedures in place for responding to situations in which:

(a) a child may have been abused or neglected or is at risk of abuse or neglect
(b) a member of staff has behaved in a way that has, or may have harmed a child or that indicates they would pose a risk of harm.

3. THE DESIGNATED SENIOR PERSON
N.B. Keeping Children Safe in Education, DfE 2016 refers to this role as Designated Safeguarding Lead - DSL

Governing bodies and proprietors should ensure that the school or college designates an appropriate senior member of staff to take lead responsibility for child protection. This person should have the status and authority within the school to carry out the duties of the post including committing resources and, where appropriate, supporting and directing other staff.

During term time the designated safeguarding lead and or a deputy will always be available (during school or college hours) for staff in the school or college to discuss any safeguarding concerns and individual arrangement for out of hours/out of term activities will be: (individual school needs to outline these below):

_____

_____

The Designated Senior Person for Child Protection in this school is:

NAME: **Sue Mansfield (Batford Nursery School), Pat Everett (Harpenden and Rural CC Group) Jo Hobbs, (Skylarks Day Care Ltd)**
There should be a Deputy Designated Senior Person (DDSP) in the absence of the lead DSP.

The Deputy Designated Senior Person for Child Protection in this school is:

NAME: Sarah Hedges **(Batford Nursery School), Julie Lannon, (Harpenden and Rural CC Group) Nicola Mainwaring, (Skylarks Day Care Ltd)**

The broad areas of responsibility for the Designated Senior Person are:

- **Managing referrals and cases**

- Refer all cases of suspected abuse or neglect to the Local Authority Children's Services (Safeguarding and Specialist Services) , Police (cases where a crime may have been committed) and to the Channel programme where there is a radicalisation concern

- Liaise with the Headteacher to inform him/ her of issues- especially ongoing enquiries under Section 47 of the Children Act 1989 and police investigations

- Act as a source of support, advice and expertise to staff on matters of safety and safeguarding and when deciding whether to make a referral by liaising with relevant agencies

- Support staff who make referrals

- Share information with appropriate staff in relation to a child's looked after (CLA) legal status (whether they are looked after under voluntary arrangements with consent of parents or on an Interim Care Order or Care Order) and contact arrangements with birth parents or those with parental responsibility.

- Ensure they have details of the CLA's social worker and the name of the virtual school Headteacher in the authority that looks after the child.

- **Training**

The Designated Senior Person should undergo formal training every two years. The DSP should also undertake Prevent awareness training In addition to this training, their knowledge and skills should be refreshed(for example via e-bulletins, meeting other DSPs, or taking time to read and digest safeguarding developments) at least annually to:

1. Understand the assessment process for providing early help and intervention, for example through locally agreed common and shared assessment processes such

as early help assessments

2. Have a working knowledge of how local authorities conduct a child protection case conference and a child protection review conference and be able to attend and contribute to these effectively when required to do so

3. Ensure each member of staff has access to and understands the school's or college's safeguarding and child protection policy and procedures, especially new and part time staff

4. Be alert to the specific needs of children in need, those with special educational needs and young carers

5. Understand and support the school or college with regards to the requirements of the Prevent duty and are able to provide advice and support to staff on protecting children from the risk of radicalisation

6. Be able to keep detailed, accurate, secure written records of concerns and referrals

7. Obtain access to resources and attend any relevant or refresher training courses

8. Encourage a culture of listening to children and taking account of their wishes and feelings, among all staff, in any measures the school or college may put in place to protect them

- **Raising Awareness**

- The designated safeguarding person should ensure the school or college's policies are known, understood and used appropriately.

- Ensure the school or college's safeguarding and child protection policy is reviewed annually and the procedures and implementation are updated and reviewed regularly, and work with governing bodies or proprietors regarding this.

- Ensure the safeguarding and child protection policy is available publicly and parents are aware of the fact that referrals about suspected abuse or neglect may be made and the role of the school or college in this.

- Link with the Local Safeguarding Children's Board (LSCB) to make sure staff are aware of training opportunities and the latest local policies on safeguarding.

- Where children leave the school or college, ensure the file for safeguarding and any child protection information is sent to any new school /college as soon as possible but transferred separately from the main pupil file.

- Schools should obtain proof that the new school/education setting has received the safeguarding file for any child transferring and then destroy any information held on the child in line with data protection guidelines (see Record keeping Guidance on Hertfordshire Grid for Learning for further information.)

4. THE GOVERNING BODY

Governing bodies and proprietors must ensure that they comply with their duties under legislation. They must also have regard to this guidance to ensure that the policies, procedures and training in their schools or colleges are effective and comply with the law at all times.

The nominated governor for child protection is:

NAME **Lara Davis** contact lara.davis@batfordnursery.herts.sch.uk

The responsibilities placed on governing bodies and proprietors include:

- their contribution to inter-agency working, which includes providing a coordinated offer of early help when additional needs of children are identified

- ensuring that an effective child protection policy is in place, together with a staff behaviour policy

- ensuring staff are provided with Part One of Keeping Children Safe in Education (DfE 2016) – Appendix 1 and are aware of specific safeguarding issues

- ensuring that staff induction is in place with regards to child protection and safeguarding

- Appointing an appropriate senior member of staff to act as the Lead Designated Senior Person. It is a matter for individual schools and colleges as to whether they choose to have one or more Deputy Designated Senior Person.

- ensuring that all of the Designated Senior Persons (including deputies) should undergo formal child protection training every two years (in line with LCSB guidance) and receive regular (annual) safeguarding refreshers (for example via e-bulletins, meeting other DSPs, or taking time to read and digest safeguarding developments)

- prioritising the welfare of children and young people and creating a culture where staff are confident to challenge senior leaders over any safeguarding concerns

- **ensuring** that children are taught about safeguarding in an age appropriate way

- Ensuring appropriate filters and appropriate monitoring systems are in place to safeguard children from potentially harmful and inappropriate online material. Additional information to support governing bodies and proprietors is provided in Annex C of **Keeping Children Safe in Education(DFE 2016**)- available at http://www.thegrid.org.uk/info/welfare/child_protection/policy/national.shtml

- Having a senior board level lead to take leadership responsibility for the organisation's safeguarding arrangements

5. WHEN TO BE CONCERNED

A child centred and coordinated approach to safeguarding:

Safeguarding and promoting the welfare of children is **everyone's responsibility.** In order to fulfil this responsibility effectively, all professionals should make sure their approach is **child centred**. This means that they should consider, at all times, what is in the best interests of the child.

Schools and colleges and their staff form part of the wider safeguarding system for children. This system is based on the principle of providing help for families to stay together where it is safe for the children to do so, and looking at alternatives where it is not, whilst acting in the **best interests** of the child at all times**...**

Children who may require early help

Families first is Hertfordshire's programme of early help services for families.
A directory of early help services is available at **www.hertfordshire.gov.uk/familiesfirst** and will help practitioners and families find information and support to prevent escalation of needs and crisis.

All staff should be aware of the **early help process**, and understand their role in identifying emerging problems, sharing information with other professionals to support early identification and assessment of a child's needs. It is important for children to receive the right help at the right time to address risks and prevent issues escalating. This also includes staff monitoring the situation and feeding back to the Designated Senior Person any ongoing/escalating concerns so that consideration can be given to a referral to Children's Services (Safeguarding and Specialist Services) if the child's situation doesn't appear to be improving.

Staff and volunteers working within the School should be alert to the potential need for early help for children also who are more vulnerable. For example:

- **Children with a disability and/or specific additional needs.**
- **Children with special educational needs.**
- **Children who are acting as a young carer.**
- **Children who are showing signs of engaging in anti-social or criminal behaviour.**

- **Children whose family circumstances present challenges, such as substance abuse, adult mental health or learning disability, domestic violence**

- **Children who are showing early signs of abuse and/or neglect.**

School staff members should be aware of the main categories of maltreatment: **physical abuse, emotional abuse, sexual abuse and neglect**. They should also be aware of the indicators of maltreatment and **specific safeguarding issues** so that they are able to identify cases of children who may be in need of help or protection.

See Appendix 4 for information on indicators of abuse and Appendix 1 for specific safeguarding issues.

Children with special educational needs and disabilities:

Additional barriers can exist when recognising abuse and neglect in this group of children.

This can include:

- Assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's impairment without further exploration;

- Assumptions that children with SEN and disabilities can be disproportionally impacted by things like bullying- without outwardly showing any signs;

- Communication barriers and difficulties

- Reluctance to challenge carers , (professionals may over empathise with carers because of the perceived stress of caring for a disabled child)

- Disabled children often rely on a wide network of carers to meet their basic needs and therefore the potential risk of exposure to abusive behaviour can be increased.

- A disabled child's understanding of abuse.

- Lack of choice/participation

- Isolation

Peer on peer abuse

Education settings are an important part of the inter-agency framework not only in terms of evaluating and referring concerns to Children's Services and the Police, but also in the assessment and management of risk that the child or young person may pose to themselves and others in the education setting.

If one child or young person causes harm to another, this should not necessarily be dealt with as abuse. When considering whether behaviour is abusive, it is important to consider:

- Whether there is a large difference in power (for example age, size, ability, development) between the young people concerned; or
- whether the perpetrator has repeatedly tried to harm one or more other children; or
- Whether there are concerns about the intention of the alleged perpetrator.

Peer on peer abuse can manifest itself in many ways and different gender issues can be prevalent. Severe harm may be caused to children by abusive and bullying behaviour of other children, which may be physical, sexual or emotional and can include gender based violence/ sexual assaults, sexting, teenage relationship abuse, peer-on-peer exploitation, serious youth violence, sexual bullying or harmful sexual behaviour.

Hertfordshire County Council recommends that education settings use The Sexual Behaviours Traffic Light Tool by the Brook Advisory Service to help professionals; assess and respond appropriately to sexualised behaviour. The traffic light tool can be found at **www.brook.org.uk/our-work/the-sexual-behaviours-traffic-light-tool.**

Guidance on responding to and managing sexting incidents can be found at:

http://www.thegrid.org.uk/info/welfare/child_protection/reference/index.shtml#sex

Staff should recognise that children are capable of abusing their peers and should not be tolerated or passed off as "banter" or "part of growing up".

In order to minimise the risk of peer on peer abuse the school:

- Provides a developmentally appropriate PSHE curriculum which develops students understanding of acceptable behaviour and keeping themselves safe.
- Have systems in place for any student to raise concerns with staff, knowing that they will be listened to, believed and valued.
- Develop robust risk assessments where appropriate (e.g. Using the Risk Assessment Management Plan and Safety and Support Plan tools).
- Have relevant policies in place (e.g. behaviour policy).

6. DEALING WITH A DISCLOSURE

If a child discloses that he or she has been abused in some way, the member of staff / volunteer should:

- Listen to what is being said without displaying shock or disbelief
- Accept what is being said
- Allow the child to talk freely
- Reassure the child, but not make promises which it might not be possible to keep
- Never promise a child that they will not tell anyone - as this may ultimately not be in the best interests of the child.
- Reassure him or her that what has happened is not his or her fault
- Stress that it was the right thing to tell
- Listen, only asking questions when necessary to clarify
- Not criticise the alleged perpetrator
- Explain what has to be done next and who has to be told
- Make a written record (see Record Keeping)
- Pass the information to the Designated Senior Person without delay

Support

Dealing with a disclosure from a child, and safeguarding issues can be stressful. The member of staff/volunteer should, therefore, consider seeking support for him/herself and discuss this with the Designated Senior Person.

If a school /college staff member receives a disclosure about potential harm caused by another staff member, they should see section 11 of this policy– *Allegations involving school staff/volunteers.*

7. RECORD KEEPING

All concerns, discussions and decisions made and the reasons for those decisions should be recorded in writing. If in doubt about recording requirements staff should discuss with the designated safeguarding lead.

When a child has made a disclosure, the member of staff/volunteer should:

- Record as soon as possible after the conversation. Use the school record of concern sheet wherever possible. (pro-forma available on the Hertfordshire Grid for Learning)

- Do not destroy the original notes in case they are needed by a court

- Record the date, time, place and any noticeable non-verbal behaviour and the words used by the child

- Draw a diagram to indicate the position of any injuries

- Record statements and observations rather than interpretations or assumptions

All records need to be given to the Designated Senior Person promptly. No copies should be retained by the member of staff or volunteer.

The Designated Senior Person will ensure that all safeguarding records are managed in accordance with the Education (Pupil Information) (England) Regulations 2005.

If a pupil who is/or has been the subject of a child protection plan changes school, the Designated Senior Person will inform the social worker responsible for the case and transfer the appropriate records to the Designated Senior Person at the receiving school, in a secure manner, and separate from the child's academic file.

8. CONFIDENTIALITY

Safeguarding children raises issues of confidentiality that must be clearly understood by all staff/volunteers in schools.

- All staff in schools, both teaching and non-teaching staff, have a responsibility to share relevant information about the protection of children with other professionals, particularly the investigative agencies (Children's Services: Safeguarding and Specialist Services and the Police).

- If a child confides in a member of staff/volunteer and requests that the information is kept secret, it is important that the member of staff/volunteer tell the child in a manner appropriate to the child's age/stage of development that they cannot promise complete confidentiality – instead they must explain that they may need to pass information to other professionals to help keep the child or other children safe. This may ultimately not be in the best interests of the child.

- Staff/volunteers who receive information about children and their families in the course of their work should share that information only within appropriate professional contexts.

9. SCHOOL PROCEDURES

Please see Appendix 3: What to do if you are worried a child is being abused: flowchart.

If any member of staff is concerned about a child he or she must inform the Designated Senior Person. The Designated Senior Person will decide whether the concerns should be referred to Children's Services: Safeguarding and Specialist Services. If it is decided to make a referral to Children's Services: Safeguarding and Specialist Services this will be discussed with the parents, unless to do so would place the child at further risk of harm.

While it is the DSPs role to make referrals, any staff member can make a referral to Children's Services. If a child is in immediate danger or is at risk of harm (e.g. concern that a family might have plans to carry out FGM), a referral should be made to Children's Services and/or the Police immediately. Where referrals are not made by the DSP, the DSP should be informed as soon as possible.

If a **teacher** (persons employed or engaged to carry out teaching work at schools and other institutions in England) , in the course of their work in the profession, discovers that an act of Female Genital Mutilation (FGM) appears to have been carried out on a girl under the age of 18 the **teacher** must report this to the police. **This is a mandatory reporting duty.** See Appendix 1- Keeping Children Safe in Education (DfE 2016): Annex A for further details.

Hertfordshire Children's Services (including out of hours) 0300 123 4043.
If the allegations raised are against other children, the school should follow section 4.3 of the Hertfordshire Safeguarding Children Board Procedures Manual – Children Who Abuse Others. Please see the school's anti-bullying policy for more details on procedures to minimise the risk of peer on peer abuse.

The member of staff must record information regarding the concerns on the same day. The recording must be a clear, precise, factual account of the observations. (Record of concern pro-forma is available on the Hertfordshire Grid for Learning).

Particular attention will be paid to the attendance and development of any child about whom the school has concerns, or who has been identified as being the subject of a child protection plan and a written record will be kept.

If a pupil who is/or has been the subject of a child protection plan changes school, the Designated Senior Person will inform the social worker responsible for the case and transfer the appropriate records to the Designated Senior Person at the receiving school, in a secure manner, and separate from the child's academic file.

The Designated Senior Person is responsible for making the senior leadership team aware of trends in behaviour that may affect pupil welfare. If necessary, training will be arranged.

10. COMMUNICATION WITH PARENTS

Batford Nursery School will ensure the Child Protection Policy is available publicly either via the school website or by other means.

Parents should be informed prior to referral, unless it is considered to do so might place the child at increased risk of significant harm by:

- The behavioural response it prompts e.g. a child being subjected to abuse, maltreatment or threats / forced to remain silent if alleged abuser informed;
- Leading to an unreasonable delay;
- Leading to the risk of loss of evidential material;

(The school may also consider not informing parent(s) where this would place a member of staff at risk).

Ensure that parents have an understanding of the responsibilities placed on the school and staff for safeguarding children.

11. ALLEGATIONS INVOLVING SCHOOL STAFF/VOLUNTEERS

An allegation is any information which indicates that a member of staff/volunteer may have:

- Behaved in a way that has, or may have harmed a child
- Possibly committed a criminal offence against/related to a child
- Behaved towards a child or children in a way which indicates s/he would pose a risk of harm if they work regularly or closely with children

This applies to any child the member of staff/volunteer has contact within their personal, professional or community life.

What school staff should do if they have concerns about safeguarding practices within the school or college

All staff and volunteers should feel able to raise concerns about poor or unsafe practice and potential failures in the school or education setting's safeguarding arrangements. Appropriate whistleblowing procedures, which are suitably reflected in staff training and staff behaviour policies, should be in place for such concerns to be raised with the school or college's senior leadership team.

If staff members have concerns about another staff member then this should be referred to the Headteacher or Principal. Where there are concerns about the Headteacher or Principal, this should be referred to the Chair of Governors/ Chair of the Management Committee/Proprietor as appropriate.

The Chair of Governors in this school is:

NAME: Juliette Barker
CONTACT : juliette.barker@batfordnursery.herts.sch.uk

In the absence of the Chair of Governors, the Vice Chair should be contacted. The Vice Chair in this school is:

NAME: Georgina Wesley
CONTACT NUMBER: contact georgina.wesley@batfordnursery.herts.sch.uk

In the event of allegations of abuse being made against the Headteacher, where the Headteacher is also the sole Proprietor of an independent school or where a staff member feels unable to raise an issue with their employer or feels that their genuine concerns are not being addressed, allegations should be reported directly to the Local Authority Designated Officer (LADO). Staff may consider discussing any concerns with the Designated Senior Person if appropriate make any referral via them. (See Keeping Children Safe in Education: Part Four, DfE 2016, for further information).

The person to whom an allegation is first reported should take the matter seriously and keep an open mind. S/he should not investigate or ask leading questions if seeking clarification; it is important not to make assumptions. Confidentiality should not be promised and the person should be advised that the concern will be shared on a 'need to know' basis only.

Actions to be taken include making an immediate written record of the allegation using the informant's words – including time, date and place where the alleged incident took place, brief details of what happened, what was said and who was present. This record should be signed, dated and immediately passed on to the Headteacher.

The recipient of an allegation must **not** unilaterally determine its validity, and failure to report it in accordance with procedures is a potential disciplinary matter.

The Headteacher/Chair of Governors will not investigate the allegation itself, or take written or detailed statements, but will assess whether it is necessary to refer the concern to the Local Authority Designated Officer:

Children's Services – 03001234043
SOOHS (Out of Hours Service-Children's Services) – 03001234043

If the allegation meets any of the three criteria set out at the start of this section, contact should always be made with the Local Authority Designated Officer without delay.

If it is decided that the allegation meets the threshold for safeguarding, this will take place in accordance with section 4.1 of the Hertfordshire Safeguarding Children Board Inter-agency Child Protection and Safeguarding Children Procedures.

If it is decided that the allegation does not meet the threshold for safeguarding, it will be handed back to the employer for consideration via the school's internal procedures.

The Headteacher should, as soon as possible, **following briefing** from the Local Authority Designated Officer inform the subject of the allegation.

For further information see:
HSCB Inter-agency Child Protection and Safeguarding Children Procedures (Electronic) Section 4.1 Managing Allegations Against Adults who work with Children and Young People

Where a staff member feels unable to raise an issue with their employer/through the whistleblowing procedure or feels that their genuine concerns are not being addressed, other whistleblowing channels may be open to them:

- Children's Services 0300 123 4043
- NSPCC whistleblowing helpline is available for staff who do not feel able to raise concerns regarding child protection failures internally. Staff can call: 0800 028 0285 – line is available from 8:00 AM to 8:00 PM, Monday to Friday and Email: help@nspcc.org.uk

Safer working practice

To reduce the risk of allegations, all staff should be aware of safer working practice and should be familiar with the guidance contained in the staff handbook/ school code of conduct / staff behaviour policy and Safer Recruitment Consortium document ***Guidance for safer working practice for those working with children and young people in education settings (September 2015)*** available at http://www.thegrid.org.uk/info/welfare/child_protection/allegations/safe.shtml

The document seeks to ensure that the responsibilities of school leaders towards children and staff are discharged by raising awareness of illegal, unsafe, unprofessional and unwise
Behaviour. This includes guidelines for staff on positive behaviour management in line with the ban on corporal punishment (School Standards and Framework Act 1998). Please see the school/college's behaviour management policy for more information.

APPENDIX 1 : KEEPING CHILDREN SAFE IN EDUCATION (DfE 2016)
Part One: Information for all school staff
Annex A: Further information

On publication of this Child Protection Policy (July 2016), the May 2016 version of the statutory guidance '**Keeping Children Safe In Education'** available online, has been denoted by DfE as 'for information only'. The guidance commences on 5th September 2016. The DfE have confirmed that this guidance will be updated annually thereafter.

The existing version of the statutory guidance mentions that there will be also be updates likely before September 2016 in respect to the definition of Child Sexual Exploitation and also regulations relating to Children Missing from Education.

The CPSLO Service have therefore decided to provide the hyperlink only to Keeping Children Safe in Education in this policy rather than the document in its entirety, due to likely frequent change in content.

It is **essential** that **all** staff have access to this online document and read Part 1 and Annex, which provides further information on:

-children missing from education
- child sexual exploitation
-'honour based' violence
-FGM mandatory reporting duty
-forced marriage
- preventing radicalisation

This is to assist staff to understand and discharge their role and responsibilities as set out in this guidance.

We highly recommend that staff are asked to sign to say they have read these sections (please see Appendix 2) and should subsequently be re-directed to these online documents again should any changes occur.

Link to Keeping Children Safe in Education:

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

APPENDIX 2: DECLARATION FOR STAFF
Child Protection Policy and Keeping Children Safe in Education (DfE 2016)

Batford Nursery School Academic Year 2016-17

Please sign and return to Sue Mansfield (DSL) by 9th September 2016

I, <insert name>_____ have read and am familiar with the contents of the following documents and understand my role and responsibilities as set out in these document(s):

(1) The School Child Protection Policy
(2) Part 1 and Annex A of 'Keeping Children Safe in Education' DfE Guidance, 2016
(2) The school's Whistle blowing Policy
(4) The school's Code of Professional Conduct
(5) The school's Health and Safety Policy
(6) The school's E-safety Policy
(7) The school's Administration of Medicines Policy
(8) The school's Children's safety and security on the premises Policy
(9) The school's Twitter usage Policy

I am aware that the DSPs are:

The Designated Senior Persons for Child Protection in this school is:

Sue Mansfield (Batford Nursery School), Pat Everett (Harpenden and Rural CC Group) Jo Hobbs, (Skylarks Day Care Ltd)

The Deputy Designated Senior Persons for Child Protection in this school is:

Sarah Hedges / Laura Butler (Batford Nursery School), Julie Lannon, (Harpenden and Rural CC Group) Nicola Mainwaring, (Skylarks Day Care Ltd)

I am able to discuss any concerns that I may have with them.
I know that further guidance, together with copies of the policies mentioned above, are available on the grid and on the staff shared area of Batford's Server

Signed_____

Date_____

APPENDIX 3: WHAT TO DO IF YOU ARE WORRIED A CHILD IS BEING ABUSED: ADVICE FOR PRACTITIONERS (DfE 2015)
Flowchart

APPENDIX 4: INDICATORS OF ABUSE AND NEGLECT

The framework for understanding children's needs:

Working Together to Safeguard Children (DFE, 2015)

Physical abuse ***Physical abuse may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating or otherwise causing physical harm to a child.***	
Child	
Bruises – shape, grouping, site, repeat or multiple	Withdrawal from physical contact
Bite-marks – site and size Burns and Scalds – shape, definition, size, depth, scars	Aggression towards others, emotional and behaviour problems
Improbable, conflicting explanations for injuries or unexplained injuries	Frequently absent from school
Untreated injuries	Admission of punishment which appears excessive
Injuries on parts of body where accidental injury is unlikely	Fractures
Repeated or multiple injurie	Fabricated or induced illness -
Parent	**Family/environment**
Parent with injuries	History of mental health, alcohol or drug misuse or domestic violence.
Evasive or aggressive towards child or others	Past history in the family of childhood abuse, self-harm, somatising disorder or false allegations of physical or sexual assault
Explanation inconsistent with injury	Marginalised or isolated by the community.
Fear of medical help / parents not seeking medical help	Physical or sexual assault or a culture of physical chastisement.

Over chastisement of child	

Emotional abuse	
Emotional abuse is the persistent emotional maltreatment of a child such as to cause severe and persistent adverse effects on the child's emotional development. It may involve conveying to children that they are worthless or unloved, not giving the child opportunities to express their views, 'making fun' of what they say or how they communicate - hearing the ill-treatment of another and serious bullying (including cyber bullying).	
Child	
Self-harm	Over-reaction to mistakes / Inappropriate emotional responses
Chronic running away	Abnormal or indiscriminate attachment
Drug/solvent abuse	Low self-esteem
Compulsive stealing	Extremes of passivity or aggression
Makes a disclosure	Social isolation – withdrawn, a 'loner' Frozen watchfulness particularly pre school
Developmental delay	Depression
Neurotic behaviour (e.g. rocking, hair twisting, thumb sucking)	Desperate attention-seeking behaviour
Parent	**Family/environment**
Observed to be aggressive towards child or others	Marginalised or isolated by the community.
Intensely involved with their children, never allowing anyone else to undertake their child's care.	History of mental health, alcohol or drug misuse or domestic violence.
Previous domestic violence	History of unexplained death, illness or multiple surgery in parents and/or siblings of the family
History of abuse or mental health problems	Past history in the care of childhood abuse, self-harm, somatising disorder or false allegations of physical or sexual assault
Mental health, drug or alcohol difficulties	Wider parenting difficulties
Cold and unresponsive to the child's emotional needs	Physical or sexual assault or a culture of physical chastisement.
Overly critical of the child	Lack of support from family or social network.

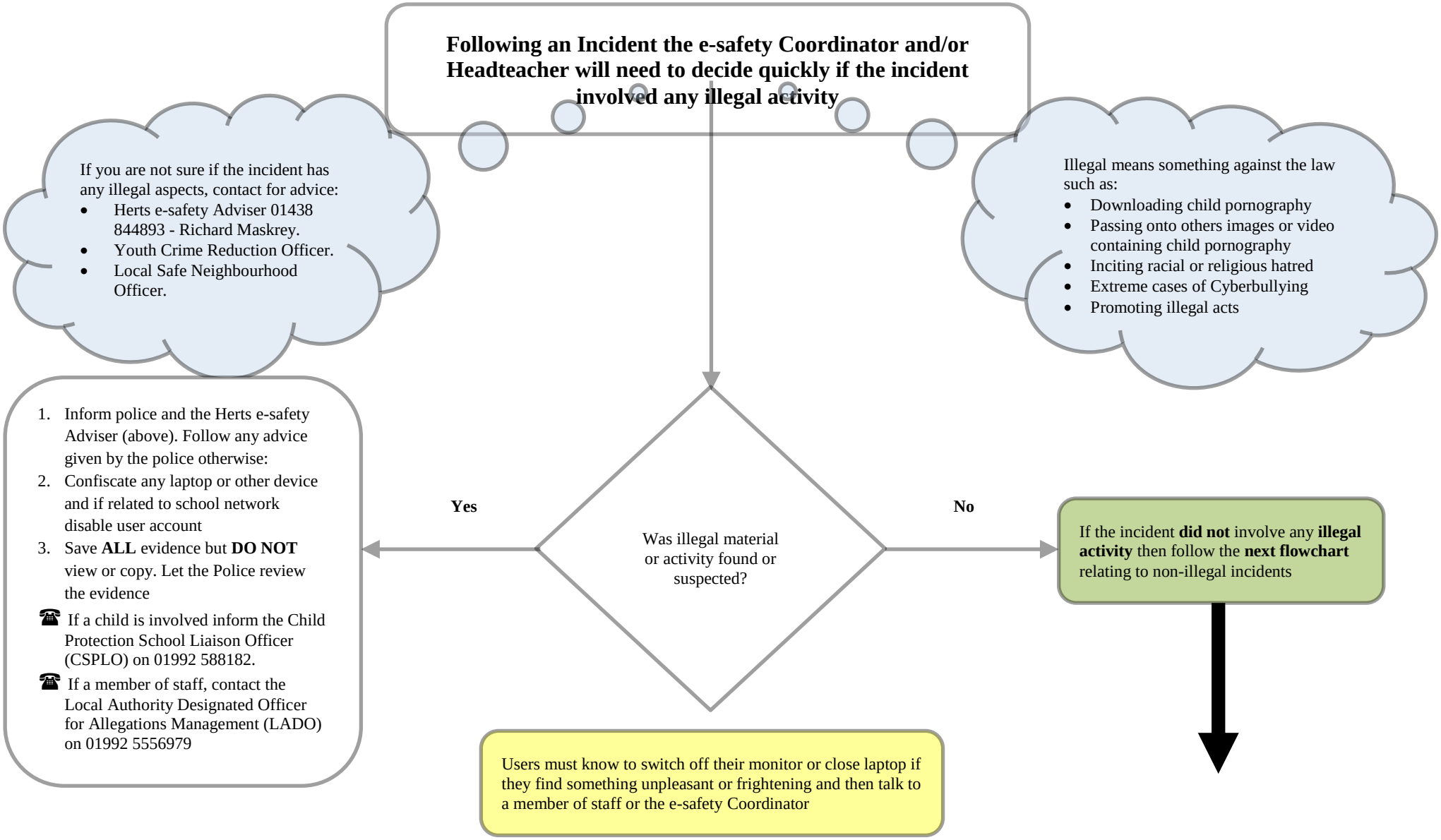
Neglect
Neglect is the persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development.

Child	
Failure to thrive - underweight, small stature	Low self-esteem
Dirty and unkempt condition	Inadequate social skills and poor socialisation
Inadequately clothed	Frequent lateness or non-attendance at school
Dry sparse hair	Abnormal voracious appetite at school or nursery
Untreated medical problems	Self-harming behaviour
Red/purple mottled skin, particularly on the hands and feet, seen in the winter due to cold	Constant tiredness
Swollen limbs with sores that are slow to heal, usually associated with cold injury	Disturbed peer relationships
Parent	**Family/environment**
Failure to meet the child's basic essential needs including health needs	Marginalised or isolated by the community.
Leaving a child alone	History of mental health, alcohol or drug misuse or domestic violence.
Failure to provide adequate caretakers	History of unexplained death, illness or multiple surgery in parents and/or siblings of the family
Keeping an unhygienic dangerous or hazardous home environment	Past history in the family of childhood abuse, self-harm, somatising disorder or false allegations of physical or sexual assault
Unkempt presentation	Lack of opportunities for child to play and learn
Unable to meet child's emotional needs	Dangerous or hazardous home environment including failure to use home safety equipment; risk from animals
Mental health, alcohol or drug difficulties	

Sexual abuse ***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 or non-contact activities, such as involving children in looking at sexual images or being groomed on line / child exploitation.***	
Child	
Self-harm - eating disorders, self-mutilation and suicide attempts	Poor self-image, self-harm, self-hatred
Running away from home	Inappropriate sexualised conduct
Reluctant to undress for PE	Withdrawal, isolation or excessive worrying

Pregnancy	Sexual knowledge or behaviour inappropriate to age/stage of development, or that is unusually explicit
Inexplicable changes in behaviour, such as becoming aggressive or withdrawn	Poor attention / concentration (world of their own)
Pain, bleeding, bruising or itching in genital and /or anal area	Sudden changes in school work habits, become truant
Sexually exploited or indiscriminate choice of sexual partners	
Parent	**Family/environment**
History of sexual abuse	Marginalised or isolated by the community.
Excessively interested in the child.	History of mental health, alcohol or drug misuse or domestic violence.
Parent displays inappropriate behaviour towards the child or other children	History of unexplained death, illness or multiple surgery in parents and/or siblings of the family
Conviction for sexual offences	Past history in the care of childhood abuse, self-harm, somatising disorder or false allegations of physical or sexual assault
Comments made by the parent/carer about the child.	Grooming behaviour
Lack of sexual boundaries	Physical or sexual assault or a culture of physical chastisement.

Hertfordshire Flowchart to support decisions related to an illegal e-safety Incident
For Headteacher teachers, Senior Leaders and e-safety Coordinators



If the incident **did not** involve and illegal activity then follow this flowchart

Hertfordshire Managing an e-safety Incident Flowchart

For Headteacher teachers, Senior Leaders and e-safety Coordinators

The e-safety Coordinator and/ or Headteacher should:

- **Record in the school e-safety Incident Log**
- **Keep any evidence**

Incident could be:

- Using another person's user name and passwor
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 0143 844767

Did the incident involve a member of staff?

Yes

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Contact the LADO on: **01992 556979** If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate) and contact school HR, Rachel Hurst or Christopher Williams on 01438 844933

No

Was the child the victim or the instigator?

Child as victim

In – school action to support child by one or more of the following:

- Class teacher
- e-safety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate

If the child is at risk inform CSPLO immediately

Confiscate the device, if appropriate.

Child as instigator

- Review incident and identify if other children were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the e-safety Coordinator

Hertfordshire Managing an e-safety Incident Flowchart involving staff as victims

For Headteacher teachers, Senior Leaders and e-safety Coordinators

All incidents should be reported to the Headteacher and/ or Governors who will:

- Record in the school e-safety Incident Log
- Keep any evidence – printouts and/ screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider including the Chair of Governors and/ or reporting the incident to the Governing Body

If you feel unable to report an incident to your HT you could talk to a member of SLT or contact the Hertfordshire e-safety Adviser 01438 844893 richard.maskrey@hertsforlearning.co.uk

Parents/ carers as instigators
Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
  - You have become aware of discussions taking place online…
  - You want to discuss this
  - You have an open door policy so disappointed they did not approach you first
  - They have signed the Home School Agreement which clearly states …
  - Request the offending material be removed.
- If this does not solve the problem:
  - Consider involving the Chair of Governors
- You may also wish to send a letter to the parent

Staff as instigator
Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools e-safety Adviser in all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Childs as instigators
Follow some of the steps below:

- Identify the child involved
- Ask child to remove offensive material. Refer to the signed Acceptable Use Agreement.

If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account

- Take appropriate actions in line with school policies/ rules
- Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Neighbourhood Team
- Anti-Bullying Adviser Karin Hutchinson 01438 844767
- If the child is at risk talk to your school DSP (Child Protection Officer) who may decide to contact LADO

Further contact to support staff include**:**

- District School Effectiveness Adviser DSEA
- Schools e-safety Adviser
- Schools HR
- School Governance
- Hertfordshire Police
- HCC Legal Helpline 01992 555536

The HT or Chair of Governors can be the single point of contact to coordinate responses.

- The member of staff may also wish to take advice from their union

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. All internet use through the HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The setting provides child's with supervised access to Internet resources (where reasonable) through the setting'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 children
- 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 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, children, 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

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid

for Learning where web-based activity is monitored and recorded

- School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml

- Batford Early Years Centre 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 are aware that setting based email and internet activity can be monitored and explored further if required

- If staff or children 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 setting, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all setting machines

- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the setting's responsibility nor the network manager's to install or maintain virus protection on personal systems

- If there are any issues related to viruses or anti-virus software, the network manager should be informed

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 staff to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of settings 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 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 a Home School agreement containing the following statement

  → **We will support the school approach to on-line safety and not deliberately 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.**

- The school disseminates information to parents relating to e-safety where appropriate in the form of;

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

Passwords and Password Security

Passwords

Please refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security

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

- **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 Headteacher immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters and numbers or symbols
- User ID and passwords for staff and children who have left the setting are removed from the system within 1 week

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use child data. Staff are expected to have secure passwords which are not shared with anyone. The children are expected to keep their passwords private and not to share with others, particularly their friends. Staff and children 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. They are also expected to use a personal password and keep it private

- 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. The automatic log-off time for the school network is ***(fill in)***

- 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)

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 mopiers (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

Please refer to the document on the grid for guidance on How to Encrypt Files

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

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

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. HCC guidance can be found:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

- With the written consent of parents and staff, the school permits the appropriate taking of images by staff and children with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of children, this includes when on field trips.
- Children and parents are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of children, staff and others without advance permission from the Headteacher
- Parents 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 Child's Images and Work

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

- in learning journals
- on the school web site and Twitter feed
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- 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
- in training materials used for staff professional development
- 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.

Childs' names will not be published alongside their image and vice versa. E-mail and postal addresses of children will not be published. Childs' 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 the designated senior leader has authority to upload to the internet.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see

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 and the specified hard drive.
- Childs and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.

- Rights of access to this material are restricted to the teaching staff and early years practitioners. The senior teachers have the responsibility of deleting the images when they are no longer required, or when the child has left the school

Webcams and CCTV

- The setting uses CCTV for security and safety. The only people with access to this are Site Supervisor and SLT. Notification of CCTV use is displayed at the front of the setting. Please refer to the hyperlink below for further guidance https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/

- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ‘ inappropriate materials’ section of this document)
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices

For further information relating to webcams and CCTV, please see **http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml**

School ICT Equipment including Portable & Mobile ICT Equipment & 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 ICT equipment to your Manager. 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 appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - 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 the setting is allowed. Our setting chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The setting allows staff to bring in personal mobile phones and devices for their

own use. Under no circumstances does the setting allow a member of staff to contact a child or parent/carer using their personal device

- The setting 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 setting community is not allowed
- Users bringing personal devices into the setting must ensure there is no inappropriate or illegal content on the device
- Personal devices must only be used during authorized breaks and only in the private areas of the building

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the setting's community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct business outside of the setting
- Never use a hand-held mobile phone whilst driving a vehicle

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 HCC and setting policies.

- Setting telephones are provided specifically for setting 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.

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**' - Page 35

- 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

Servers

- 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
- Remote backups should be automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777
- Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data. At the moment SITSS do not encrypt servers, however Office PCs (including Office Master PCs) installed by SITSS are supplied with encryption software installed

Social Media, including Facebook and Twitter

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

- Our setting uses Twitter to communicate with parents and carers. A designated member of the senior leadership team 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 any time

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

- Staff, governors, parents and carers should never use their own or others' personal social media accounts to discuss or make posts about the setting or individuals from the setting community. **The laws of slander and libel apply to social media**

Systems and Access

- You are responsible for all activity on setting systems carried out under any access/account rights assigned to you, whether accessed via the setting's 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 setting or may bring the setting or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the setting'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 setting systems, hardware or used in relation to setting 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 a 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.

Further help and support

Your 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 2014. 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/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf

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 e-safety

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/

Appendix

Information Risk Actions Form

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Writing and Reviewing this Policy

Staff and Child Involvement in Policy Creation

- Staff and governors have been involved in reviewing the Policy for ICT Acceptable Use through staff meetings and meetings of the Governing Body

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, Headteacher and governors during the 2015.