



A WHOLE SCHOOL POLICY FOR E-Safety

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

Safeguarding is a serious matter; at Frances Olive Anderson Church of England School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Frances Olive Anderson Church of England Primary School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Headteacher Name: Sarah Woolley Signed:

Chair of Governors: Signed:

Review Date: September 2016 Next Review: September 2017

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
 - Have e-safety as an agenda item at the Pupils and Staffing Sub Committee

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to Stewart Cook with Sarah Woolley as support.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

This policy must be shared with Mouchel who act as our technical staff.

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any e-safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
 - Passwords are applied correctly to all users regardless of age Passwords for staff will be a minimum of 8 characters. The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and meetings the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

E-Safety as part of Pupils and Staffing

the Governing Body is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Established from volunteer students, parents, e-Safety Officer, responsible Governor and others as required, the e-Safety Committee will meet on a termly basis.

Technology

Frances Olive Anderson Church of England School uses a range of devices including PC's, laptops, iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use mouchels software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use System Centre Endpoint Protection software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All devices are encrypted using bitlocker and encryption. All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does not mean password protected.)

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff passwords will change on a six weekly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed. Students passwords do not change

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Frances Olive Anderson Church of England Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Frances Olive Anderson Church of England Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Frances Olive Anderson Church of England Primary School will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

The e-Safety Training Programme can be found in our Five Year Safeguarding Training Pathway.

Acceptable Use Policy – Staff

Need to print off and sign

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Mouchel Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE :

DATE :

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people’s work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people’s usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

SEE NEXT PAGE FOR SAMPLE PARENTS LETTER

FRANCES OLIVE ANDERSON
Church of England (Aided) School
The Grove, Lea, Gainsborough DN21 5EP
Telephone: 01427 612827
Fax: 01427 612446
e-mail: enquiries@olive-anderson.lincs.sch.uk
of Lincoln
Website: www.olive-anderson.lincs.sch.uk
Headteacher: Mrs Sarah Woolley



Diocese

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact enquiries@olive-anderson.lincs.sch.uk

Yours Sincerely

Sarah Woolley

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –

Name of Child –

Signature -

Date

e-Safety Incident Log

Number:	Reported By: <i>(name of staff member)</i>	Reported To: <i>(e.g. Head, e-Safety Officer)</i>
	When:	When:
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		

--	--	--	--



Signature (Headteacher)		Date:	
------------------------------------	--	--------------	--



Signature (Governor)		Date:	
---------------------------------	--	--------------	--

Risk Log

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	2	3	6	e-Safety Officer IT Support
2.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	
3.	Blogging	Inappropriate comments - students	2	3	6	
4.	Blogging	Inappropriate comments – staff and parents	2	3	6	
5.	copyright	Copyright terms breached.				

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = **Low Risk**
4 – 6 = **Medium Risk**
7 – 9 = **High Risk**

Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.
Final decision rests with Headteacher and Governing Body

Risk Assessment

Risk No.	Risk
1	Access to inappropriate/illegal content - staff
Likelihood	Staff are more likely to come across inappropriate content by accident rather than actively seeking to find inappropriate content. Staff might be tempted to use school equipment for personal use at home, this is not acceptable.
2	
Impact	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a staff member accesses illegal material using school-owned equipment.
3	
Risk Assessment	6 medium risk
Risk Owner/s	e-Safety Officer / HT IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using mouchels software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet.</p> <p>The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Staff will be spoken to directly about the appropriate use of the Internet. Staff will be made aware that the laptop / I pads are for school work only. Staff are up to date about the risks involved and sign the Code of Conduct each September.</p>

Risk No.	Risk
2	Access to inappropriate/illegal content - students
Likelihood	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 2.
2	
Impact	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
3	
Risk Assessment	6 medium risk
Risk Owner/s	e-Safety Officer / HT IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using mouchels software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school.</p> <p>Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will</p>

	be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.
--	---

Risk No.	Risk
3	Blogging - Inappropriate comments - students
Likelihood 2	Some students may choose to use social media and blogging to be unkind to others through what they post or status information. Some students may become the victim of such inappropriate use of social media.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student posts inappropriate material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student. The students may be at risk of Cyber-Bullying
Risk Assessment	6 medium risk
Risk Owner/s	e-Safety Officer / HT IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using mouchels software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school.</p> <p>Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. The police will be contacted if necessary. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.</p>

Risk No.	Risk
4	Blogging - Inappropriate comments – staff / parents
Likelihood 2	Some adults may choose to use social media and blogging to be unkind to others through what they post or status information. Some adults may become the victim of such inappropriate use of social media.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a staff member posts inappropriate material using school-owned equipment. There is a potentially damaging aspect to the adults. Adults may be at risk of Cyber-Bullying
Risk Assessment	6 medium risk
Risk Owner/s	e-Safety Officer / HT IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using mouchels software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the</p>

	<p>Internet.</p> <p>The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Staff will be spoken to directly about the appropriate use of the Internet. Staff will be made aware that the laptop / I pads are for school work only. Staff are up to date about the risks involved and sign the Code of Conduct each September.</p> <p>The police will be notified and further support accessed in the event of inappropriate comments being made by staff or parents.</p>
--	--

Risk No.	Risk
5	Copyright terms being breached
Likelihood	All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons). Copyright
2	
Impact	The impact to the school reputation would be high.
3	
Risk Assessment	6 medium risk
Risk Owner/s	e-Safety Officer / HT IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using mouchels software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet.</p> <p>The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Staff and pupils will be spoken to directly about the appropriate use of the Internet. Staff and pupils are up to date about the risks involved and sign the Code of Conduct each September.</p> <p style="background-color: #ffff00;">Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.</p>

Approved / Not Approved (circle as appropriate)

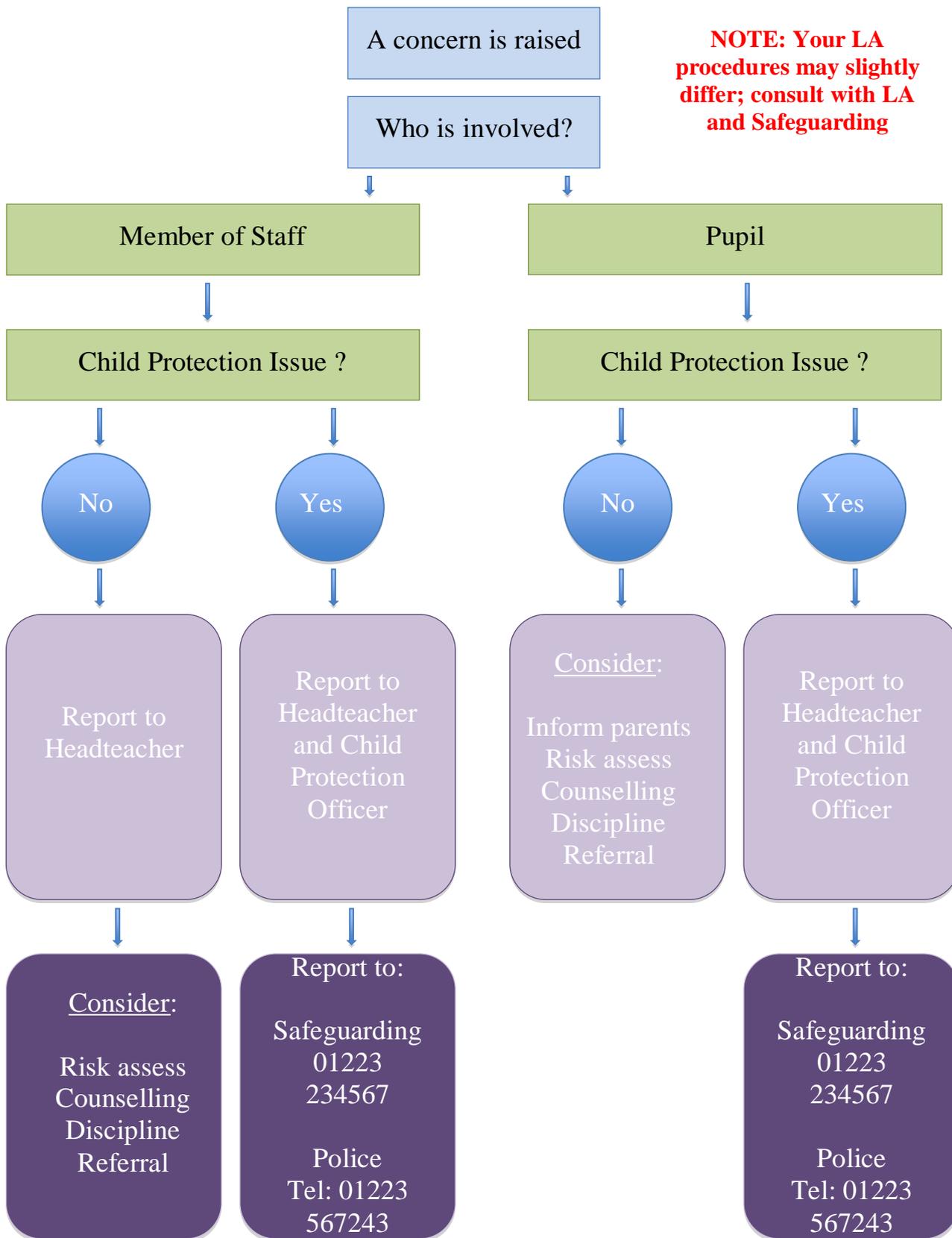
Date:

Signed (Headteacher) :

Signed (Governor) :

Inappropriate Activity Flowchart

NOTE: Your LA procedures may slightly differ; consult with LA and Safeguarding



If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding

Agreed by the Governing Body in December 2015. To be reviewed August 2016.