Updated June 2020 to include
Acceptable Use of the Internet, Digital Technology

CHILTON FOLIAT CE VA PRIMARY SCHOOL

'Of Heart and Mind'

Our School Christian Vision

With thankfulness, courage and love,
we strive to improve heart and mind.

At Chilton Foliat Primary School we honour our educational heritage, supported by a strong Christian ethos. We strive to provide a diverse education that inspires children to develop a **thirst for knowledge**. This is delivered in a safe, supportive and nurturing environment promoting self-discipline, motivation and excellence in learning.
We encourage strong partnerships and positive relationships amongst pupils, parents, carers, staff and the wider community.

Acceptable Use of the Internet, Digital Technology and E-Safety Policy

Please note that there may be Toolkits, Forms and other documents relating to this Policy which can be found on the LA HR website.
Please contact the Clerk of Governors for access to the LA HR department.

Policy waiting adoption by the Full Governing Body

Updated June 2020 to include

Acceptable Use of the Internet, Digital Technology

Introduction

Our Acceptable Use of the Internet, Digital Technology and E-Safety policy has been written in accordance with government guidance and is referenced in the School Improvement Action Plan. It relates to and should be read in conjunction with other policies including those for Child Protection, Anti-bullying, Behavior and Discipline, Data Protection and Freedom of Information, in addition to the Staff Code of Conduct for Safer Working Practice. The aim of this policy is to:

- Provide a mechanism by which all staff and children are kept safe when using any form of internet or digital technology provided by the school
- Allow all users access to school digital resources and the use of the Internet for educational purposes
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data inschools
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with our behavior policy and etiquette
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school
- It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

General Internet Use and Consent

- Children who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material
- The use of the names of children or photographs of children for websites will require written permission from parent(s)/carer(s) included on the photographic consent form. If a picture is placed on the website the child's full name will not be displayed
- If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Heateacher immediately who will, in turn, record the address and report on to the schools and Internet Service Provider, via their technical support
- Children are aware that they must only access those services they have been given permission to use. Staff and children are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)
- Staff are discouraged from being members of social networking sites. However, if staff are members, they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/children or ex-children) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises child or staff confidentiality will be classed as a disciplinary matter.
- Staff and Governors must agree to and sign the Acceptable Use Agreement (appendix) each year. Children and parent(s)/carer(s) must agree to and sign the Acceptable Use Agreement

on entry to the school. * Exceptional provision is being made for acknowledgement for Acceptable Use in the current COVID-19 crisis.

Effective E-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband including the effective management of Websense filtering.

Teaching and Learning

Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems
- The school Internet access designed expressly for pupil use and includes filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be regularly informed about E-Safety through planned whole school and class instruction and as an ongoing aspect of the computing curriculum
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Any work or activity on the Internet or school equipment must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden
- Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by children and staff as they can result in degradation of service for other users and increase the workload of the IT staff.
- Users must not download, use or upload any material that is subject to copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material. Users should assume that ALL software is subject to copyright restrictions, including shareware.
- Children must not, under any circumstances download or attempt to install any software on the school computers, Chrome Books or tablets. Staff should seek the advice of the Headteacher before attempting to download or upload software. Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.
- All children are aware of procedures to report any incidents of sexual or inappropriate content, radicalisation, extremism or anything else that worries them, which they encounter during use of the Internet. The school will react appropriately and work with children, parents and any other appropriate authority to resolve the issue. (Perhaps worth referring to where this procedure can be found our outlining it?)

Updated June 2020 to include
Acceptable Use of the Internet, Digital Technology

Log in and Passwords

- Children and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account. Note: The primary user of Microsoft Teams will be the parent, not the child and will therefore take ultimate responsibility when using Microsoft Teams at home
- Children and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password
- Staff and children must ensure Prowise boards, laptops, iPads or Chrome Books are logged off (or hibernated) when left unattended
- All staff Prowise Boards, iPads and laptops will have a uniform password that is shared only with members of staff
- Adult users are expected to manage their own areas on the network where relevant. Passwords are therefore set for each user in these circumstances. We recommend that passwords are changed regularly.

Mobile Devices

Pupils are not permitted to bring a mobile device to school.
Staff should only use their mobile phones at appropriate times of the day only e.g. break times when there are no children present.
During the school day their mobiles should be turned off or set to silent and put away in line with Safeguarding measures.
Staff must not use personal mobile devices or cameras to take images of children or staff.
Acceptable emergency use:

1. School trips where staff may need to contact school or a member of senior leadership team
2. Occasions where staff need to take photos on a phone but must instantly delete / send across and show another staff member that this has happened
3. Emergency incident on site where a member of senior leadership is needed.

Video-Conferencing and Webcams

- Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups **outside** of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

School Network and Child Files

- Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area. Where provision allows, children can access and save work to their own log-on through the server; this can only be accessed by that child, the class teacher, the Computing Leader and the IT support.
- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask their teacher or IT Support for advice.

Updated June 2020 to include

Acceptable Use of the Internet, Digital Technology

- Users accessing software or any services available through school facilities must comply with license agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the network is accessed from home, this Acceptable Use Policy applies.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly.

Email or other inter-computer transactions

Use of email and communication by email should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. Email can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if it appears to be deleted from the computer.

When using email, children and staff should:

- Not access personal emails in school using school equipment
- Be aware that email is not a secure form of communication and therefore children should not send ANY personal information
- Not open email attachments from unknown senders or from computers from which virus protection may not be current or activated
- Not send email messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive
- Not open email attachments from unknown senders or from computers from which virus protection may not be current or activated

This Guidance will apply to any inter-computer transaction, be it through web services, chat rooms, bulletin and news groups, blogging or peer to peer sharing.

Published content and the school web site

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the webssite, particularly in association with photographs
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website. A Permission Register is maintained by the school office

Social networking and personal publishing

- The school will block/filter access to social networking sites
- Pupils are advised never to give out personal details of any kind which may identify them or their location

- Pupils and parents are advised that the use of social network spaces (e.g. Facebook) outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed regularly and improved where necessary
- If staff or pupils discover an unsuitable site, it must be reported to the DSL (Designated Safeguarding Lead) as soon as possible using Appendix 3 (they will have the site blocked).

Managing emerging technologies

- As the quantity and breadth of information available via the Internet continues to grow it is not possible to guard against every undesirable situation. The school will take all reasonable precautions to ensure that pupils only access appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, nor Wiltshire Council can accept liability for the material accessed, or any consequences of internet access
- Methods to identify, assess and minimise risks will be reviewed regularly
- The Headteacher will ensure that the Acceptable Use of the Internet, Digital Technologies and E Safety Policy is implemented and compliance with the policy is monitored
- Our pupils may not bring mobile phones to school. If a pupil is found in possession of a mobile phone, it will be handed in to the school office.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. Refer to the school's Data Protection Policy at the school website http://www.chiltonfoliatprimary.org.uk/

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Parents and pupils will need to work in partnership with staff to resolve issues (refer to our Data Protection policy link above), and the school's complaints procedure followed should further escalation be necessary for resolution.

Staff and the Acceptable Use of the Internet, Digital Technologies and E-Safety policy

- All staff will be given the School Acceptable Use of the Internet, Digital Technologies and E-Safety Policy and Social Networking Policies and their importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff MUST talk to their class about e-safety rules at the start of the year and remind them at least each term
- Any email sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted
- Members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Off-site child data and child information

- Laptops and back-ups (USB sticks/external hard drives) may be taken off site where agreed with the Computing Leader or Headteacher. These should have encryption/security measures in place to prevent data being accessed in the event of loss or theft
- Staff are to ensure that laptops are used cautiously when viewing child data/information and images and that laptops are logged off when left unattended. Images must be transferred to the school network as soon as possible and be removed within the set timescales.
- Data, images and child information must be removed from backups and laptops when children transfer to another class to avoid records being kept of children that are not taught by their former teacher.

Children with Additional Learning Needs

- The school strives to provide access to a broad and balanced curriculum for all pupils and recognises the importance of tailoring activities to suit the educational needs of each child. Where a child has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and Internet access.
- Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).
- Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable UseAgreement.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- Regular information will be provided to parents about how they can work with the school to keep their children safe and ensure this resource is used appropriately both within school and at home.

Cyberbullying

For most, using the Internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that pupils, staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond to and combat misuse.

Preventing Cyberbullying

- The best way to deal with Cyberbullying is to prevent it happening in the first place.

Understanding and talking about cyberbullying

- The whole school community needs a shared, agreed definition of cyberbullying. Everyone needs to be aware of the impact of cyberbullying and the ways in which it differs from other forms of bullying.

Making reporting cyberbullying easier

- All cyberbullying incidents will be properly recorded and investigated using E-Safety Incident Log Form to be submitted to the DSL (Designated Safeguarding Lead (see appendix)

Responding to Cyberbullying

Supporting the person being bullied:

- Give reassurance that the person has done the right thing by telling someone, refer to any existing pastoral support/procedures and inform parents.

Advise on next steps:

- Make sure the person knows not to retaliate or return the message
- Help the person to keep relevant evidence for any investigation (e.g. by not deleting messages they have received, and by taking screen capture shots and noting web addresses relating to online cyberbullying instances).
- Check the person understands simple ways to prevent it from happening again, e.g. by changing contact details
- In cases of illegal content, contact the police, who can determine what needs to be kept for evidential purposes.

Investigating Incidents

All cyberbullying incidents will be properly recorded and investigated using an E-Safety Incident Log Form (see Appendix 3)

- Advise pupils and staff to keep a record of the bullying as evidence
- Take steps to identify the bully, including looking at the school systems, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. The police will need to be involved to enable the service provider to look into the data of another user. (See Anti bullying Policy)
- Once the person bullying is identified, steps will be taken to change their attitude and behaviour as well as ensuring access to any support that is required.
- Evaluating the impact of prevention activities

Regular reviews are vital to make sure that anti-bullying policies are working and are up to date.

This policy will feature as part of the process within the school Improvement Plan. It has been agreed by all staff and approved by the governors. It will be reviewed annually.

APPENDIX 1

Acceptable Use of the Internet, Digital Technologies and E-Safety Policy – **Staff Agreement**

1. All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the Internet, email or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.
2. I know that I must only use the school equipment in an appropriate manner and for professional uses. I understand that I need to obtain the permission of parents/guardians for children and young people before they can upload images (video or photographs) to the Internet or send them via email.
3. I know that images should not be inappropriate or reveal any personal information of children and young people.
4. I have read the procedures for incidents of misuse in the Internet and Digital Technology Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
5. I will report accidental misuse.
6. I will report any incidents of concern for a child or young person's safety to the Designated Safeguarding Lead or Headteacher in accordance with procedures listed in the Acceptable Use Policy.
7. I know who my Designated Safeguarding Lead is.
8. I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal email. I know I should use the school email address and phones to contact parents.
9. I know that I must not use the school system for personal use unless this has been agreed by the Headteacher.
10. I know that I should complete virus checks on my laptop and other storage devices; including regularly installing updates on to school devices, so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
11. I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
12. I will ensure that I keep my password secure and will not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Headteacher prior to sharing this information.
13. I will adhere to copyright and intellectual property rights.
14. I will only install hardware and software I have been given permission for.
15. I will ensure the safe keeping of school equipment if I take it off of the school premise and will ensure devices are encrypted/security protected to prevent access to data in the event of loss or theft. I will be responsible for loss, theft and damage.
16. I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
17. I have been shown a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow. A copy can be found on the school website.

I have read, understood and agree with these Agreements as I know that by following them I have a better understanding of e-safety and my responsibilities to safeguard children and young people when using online technologies.

Signed: _____ Dated: _____

Chilton Foliat CofE VA Primary School

APPENDIX 1

Acceptable Use of the Internet, Digital Technologies and E-Safety Policy – **Pupil/Parent Agreement**

Pupils are permitted to use IT systems on the following conditions:

1. I will only use the school's equipment and ICT systems, including the Internet, email, digital video, mobile technologies, etc. for school purposes.
2. I will not download or install software on school technologies.
3. I will only log on to the school network/ Learning Platform with my own user name and password.
4. I will follow the schools ICT security system and not reveal my passwords to anyone and will change them regularly.
5. I will only use my school email address.
6. I will make sure that all ICT communications with pupils, teachers or others are responsible and sensible.
7. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
8. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
9. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
10. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
11. I will respect the privacy and ownership of others' work on-line at all times.
12. I will not attempt to bypass the Internet filtering system.
13. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available on request to teachers.
14. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer will be contacted.

Parent/Carer signature …… Child signature ……..

Child's Name …… Class …… Date ……..

APPENDIX 1 - E-Safety Audit

The school will be aware of **all** the sensitive data it holds, be it electronic or on paper.

- A register will be kept detailing the types of sensitive data held, where and by whom (refer to the '**Data Protection Policy'** document '**Appendix 4. Register of Sensitive data held by the School')**, and will be added to as and when new data is generated.
- How long these documents need to be kept will be assessed using the Records Management Toolkit.
- Audits will take place every two years, or as necessary.
  Note: *The DfE's own statutory guidance recommends reviewing data protection / E-Safety annually, even though their own Data Protection policy template specifies a 2 year review period. In view of this ambiguity, CFPS have decided to review annually, see below).*

- This register will be sent to all staff each year to allow colleagues to revise the list of types of data that they hold and manage.

- The audit will be completed by a member of staff responsible for data protection.

APPENDIX 2 – E-Safety Advice

E-safety tips for Parents of Primary School Children

79% of 7-11 year-olds said they would tell their parent or carer if something worried them online.

Childnet, Have your Say (2013)

Checklist

Put yourself in control
Make use of the parental controls on your home broadband and any internet-enabled devices. You can find out how at your broadband provider's website or by visiting internetmatters.org.

Search safely
Use safe search engines such as swiggle.org.uk or kids-search.com. Safe search settings can also be activated on Google and other search engines as well as YouTube. You can find out more at google.co.uk/safetycentre.

Agree boundries
Be clear what your child can and can't do online – where they can use the internet, how much time they can spend online, the sites they can visit and the type of information they can share. Agree with your child when they can have a mobile phone or tablet.

Explore together
The best way to find out what your child is doing online is to ask them to tell you about it. Put the family computer in a communal area so you can see what sites they're visiting and share with them.

Check if it's suitable
The age ratings that come with games, apps, films and social networks are a good guide to whether they're suitable for your child. The minimum age limit is 13 for several social networking sites, including Facebook and Instagram.

Know this stuff matters, but don't know where to turn?

Internet Matters is a free online resource for every parent in the UK. We'll show you the best ways to protect your children online – with information, advice and support on all the big e-safety issues.

internet matters.org

Learn about it:

Teach your child some simple rules

- Make sure your child knows not to share personal information like their phone number or email address online
- Only talk to real life friends or family if they are on sites with a social media element like Moshi Monsters or Club Penguin
- Use privacy settings wherever they exist to keep their information private
- Be a good online friend and don't say nasty things even if it's just a joke
- Use secure and legal sites to download music and games
- Check attachments and pop ups for viruses before they click or download anything
- Use Public Friendly WiFi when they're out and about to filter inappropriate content

Talk about it:

Tips for a meaningful conversation

- Start conversations when your children won't be embarrassed, for example in the car going home from school
- Ask them for advice on how to do something online and use this as a conversation starter
- Make sure they know they can come to you if they're upset by something they've seen online
- Be sensitive and praise them when they share their online experiences with you
- If your child comes to you with an issue, stay calm and listen without judging them
- Talk about online grooming as you would stranger danger and explain that people they meet online might not be who they say they are

Deal with it:

You can find out where to get help and advice on the Take Action page of internetmatters.org, where we include information on how to report problems – and which relevant organisations and agencies to turn to.

On this page, we also provide information on how to deal with any specific issues you may encounter with your child; such as finding inappropriate content and cyberbullying.

Stay safe at secondary school

Exposure to some of these issues increases when children move up to secondary school so make sure your child is prepared – find out more with our pre-teens age guide at **internetmatters.org/ageguide10-13**

internet matters.org

E-safety tips for Parents of Pre-School Children

81% of mothers have uploaded an image of their child under 2 to social media sites

Zero to eight: Young children and their internet use – EU Kids Online (August 2013)

Checklist

☑ **Put yourself in control**
Make use of the parental controls available on your home broadband and any internet-enabled devices. You can find out how at your broadband provider's website or by visiting internetmatters.org.

☑ **Search safely**
Use safe search engines such as swiggle.org or kids-search.com. Safe search settings can also be activated on Google and other search engines as well as YouTube. You can find out more at google.co.uk/safetycentre.

☑ **Set boundaries**
It's never too early to start setting rules about when and for how long your child can use devices and start to introduce the subject of internet safety at the same time. Keep your computer in a communal area, keep other devices out of reach and use passwords so they can't go online without asking you first.

☑ **Explore together**
Set your homepage to a child-friendly site such as CBeebies and give them a user account which only allows access to sites you've chosen. Explore these different sites together.

☑ **Help them learn through games**
Games are a great way for young children to explore the internet and learn about the world around them. You can choose safe, fun and educational games free of charge from providers such as Fisher Price or about their favourite characters like Peppa Pig.

Children can now have a digital footprint before they learn to speak and often before they're even born.

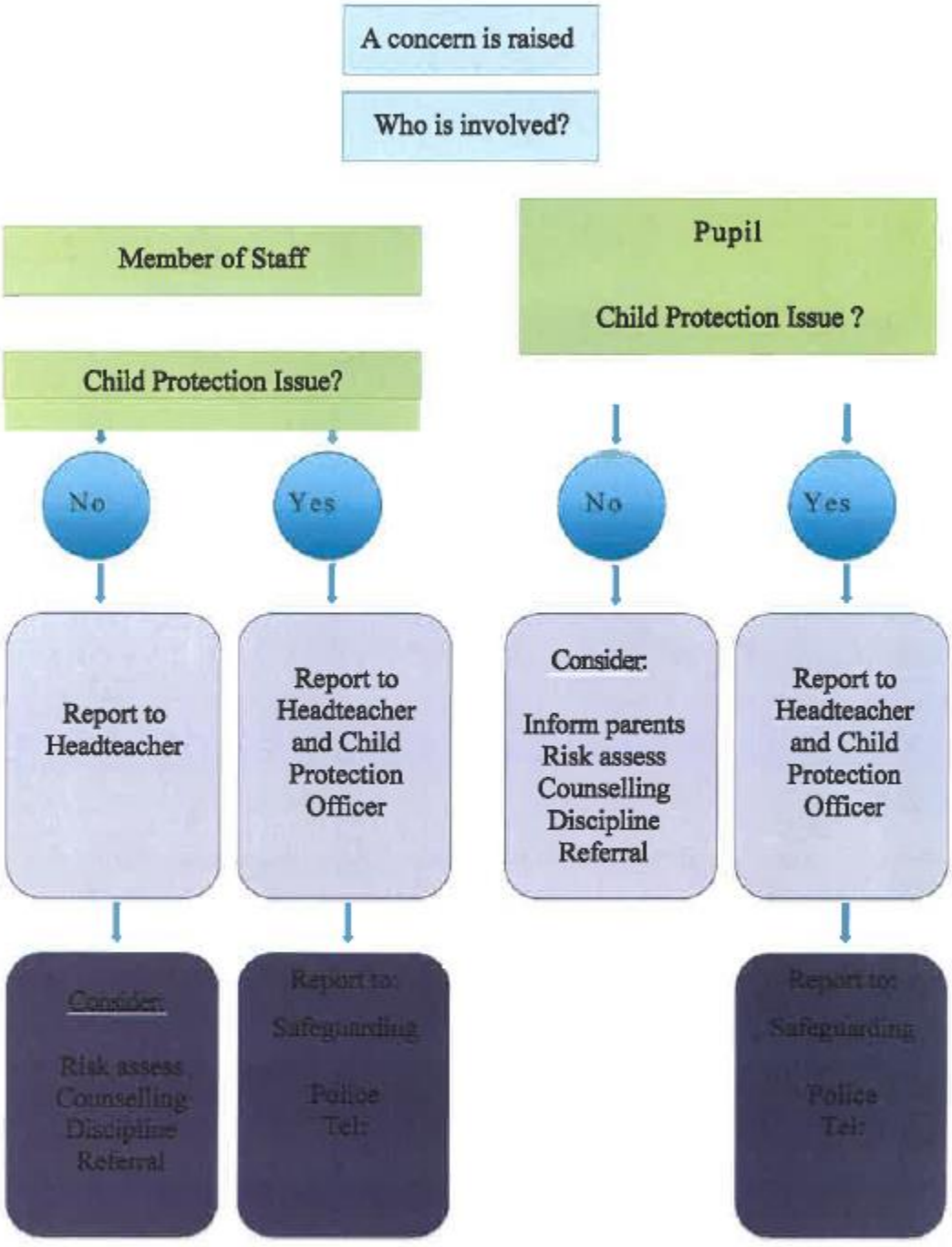
Internet Matters is a free online resource for every parent in the UK. We'll show you the best ways to protect you children online as they grow up – with information, advice and support on all the big e-safety issues.

internet matters.org

APPENDIX 3 – E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head - DSL)*
	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:**

APPENDIX 4 – Inappropriate Activity Flowchart



If you are in any doubt, consult the Headteacher, Senior Teacher, DSL/DDSL

APPENDIX 5 – Illegal Activity Flowchart