Online Safety Policy
2025 -2026

Our small school community welcomes everyone and aspires to meet the needs of all through high expectations, Christian values and compassionate support. We strive to create a firm foundation for all to fulfil their potential as future citizens of the world. Our challenging, exciting learning environment enables everyone to go forward as champions of compassion, curiosity and courage.

Jesus answered, love the Lord your God with all your heart, with all your soul, and with all your mind. This is the greatest and the most important commandment. The second most important commandment is like it: love your neighbour as you love yourself. Matthew 22:v.37-40

POLICY STATEMENT

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, pupils, governing body, school volunteers (including 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 Partney CofE Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding 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 Partney C of E Primary School website; upon review all members of staff will sign as read and understood both the Online Safety Policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupil Acceptable Use Policy will be sent home with children 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, pupils will be permitted access to school technology including the Internet.

POLICY GOVERNANCE (ROLES & RESPONSIBILITIES)

Aims

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

Governing Body

The governing body will:

- Review this policy annually and in response to any Online Safety incident to ensure that the policy is up-to-date, to ensure that it covers all aspects of technology use within the school, to ensure incidents were appropriately dealt with and to ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:
    - Keep up-to-date with emerging risks and threats through technology use.
    - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.

Head Teacher

Reporting to the governing body, the Head Teacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to two members of staff, the Online Safety Leaders, as indicated below.

The Head Teacher will ensure that:

- Online 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.
- The designated Online Safety Leaders have had appropriate CPD in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately and retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

Online Safety Leaders

The day-to-day duty of the Online Safety Leader is devolved to the school's Designated Safeguarding Leads and Computing Subject Leader.

The Online Safety Leaders will:

- Keep up to date with the latest risks to children whilst using technology; be familiar 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 Head Teacher.
- Work with the Head Teacher to advise the governing body on Online Safety matters.
- Engage with parents and the school community on Online Safety matters
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical Online Safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or IT Technical Support.
- Make themselves aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher and responsible governor to decide on what reports may be appropriate for viewing.

IT Technical Support Staff (ARK ICT)

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.
    - Operating system updates are regularly monitored and devices updated as appropriate.
    - Any Online 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 Online Safety Leaders and the Head Teacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
    - Passwords for pupils can be shorter to make them age-appropriate.

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 Head Teacher.
- Any Online Safety incident is reported to the Head Teacher and Online Safety Leaders (and an Online Safety Incident report is made through CPOMS). If you are unsure the matter is to be raised with the Online Safety Leaders or the Head Teacher to make a decision.
- The reporting flowcharts contained within this Online Safety policy are fully understood.

All Pupils

The boundaries of use of IT equipment and services in this school are given in the Pupil Acceptable Use Agreement, including online remote survey agreements for periods of remote learning where live video meetings take place daily; any deviation or misuse of IT equipment or services will be dealt with in accordance with the behaviour policy.

Online Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils 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 school newsletters and the school website, the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

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

Governors

Online safety will be reported on at Governors.

- Governors will be advised on changes to the Online Safety policy.
- Governors will establish the effectiveness (or not) of Online Safety training and awareness in the school.

Risk assessment of potential issues/dangers
The Online Safety Leaders will ensure that the risk assessment is kept up-to-date in line with technological developments within the school (located at the end of this policy). The risk assessment will be shared with all staff members and the school's IT technical support provider.

In the event of staff/pupils accidentally accessing online material that they deem to be inappropriate/offensive, it will be reported to the Online Safety Leader or, in their absence, to the Head Teacher.

Protection against extremism/radicalisation
Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the Internet as a means of either inciting violence against specific groups or providing information on carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.
• Appropriate filtering is in place and will be reviewed whenever there is an incident of pupils accessing websites advocating extremism;
• The Online Safety Leaders will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school or its pupils;
• A referral will be made to the police through PREVENT channel procedures whereby a pupil is involved in the extremist narrative and there is evidence that their parents are involved in advocating extremist violence.

TECHNOLOGY

Partney C of E Primary School uses a range of devices including PCs, laptops, iPads, Chrome Books, MacBooks and Nintendo DS consoles. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – The school uses a Meraki MX security appliance which is CIPA-compliant (Children's Internet Protection Act). This 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 Computing Coordinator, Online Safety Leaders, the Head Teacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher. St. Michael's school has an appropriate level of filtering on accessing the internet in school to ensure that both staff and children are safe from accessing radical and extremist material whilst using networks and devices in school.

Email Filtering – The school uses the Gmail system and Google has comprehensive virus protection, Spam filtering & Message Centre and quarantine summary. This helps prevent 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 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 drives) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. Staff will require permission from the Head Teacher to use portable storage media (USB memory sticks, discs, SD cards, etc.) on any school device. Any such device containing sensitive or pupil data must be encrypted in order to prevent GDPR breaches. (Note: Encryption does <u>not</u> mean password protected.)

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change if there has been a compromise. The Computing subject leader and IT Support will be responsible for ensuring that passwords are changed. Please note that the Nintendo DS consoles cannot be password protected. As we currently use Google Drive and sensitive data is stored online, it is imperative that Gmail passwords contain a mixture of capital and lower case letters, numbers and punctuation. There are NOT to be written down or shared with ANYONE.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated weekly during our IT technician visits. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns.

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 Online Safety and the staff Acceptable Use Policy; pupils upon receiving parental signature and returning their acceptance of the Pupil 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. Older pupils may be permitted to use the school email system, and as such will be given their own email address.

Photos and videos –All parents must sign a photo/video/social media 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; Partney C of E 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 St Michael's C of E Primary School and have been appropriately risk assessed; should staff wish to use other social media; permission must first be sought via the Online Safety Leaders who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff in school
- Twitter – used by the school
- Facebook - used by the school
- Authority to use official school social media will be given to individual members of staff by the Head Teacher

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

- Permission slips must be consulted before any image/video of any child is uploaded.
- There is to be no identification of pupils 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 license which allows for such use (i.e. creative commons).

Pupils using/accessing social networking websites and/or apps

- Under no circumstances should a child access social networking websites in school unless it is for a purpose instigated by the child's teacher. The school network system prohibits pupils from accessing these websites but the bypassing of the system or accessing through a mobile phone is strictly prohibited.
- If any reports are received of pupils making inappropriate comments about staff or other pupils, hard copies will be obtained and the child will be reported immediately (to the website host) to have their account terminated. The parents/carers of the child will also be notified and this could result in further action. If the comment is about a member of staff a referral may be made to the county's legal services.

Parents using social networking websites and/or apps

- If hard copies of inappropriate comments about members of staff, pupils within the school or school decisions are received, the matter may be referred to the county's legal services and subsequent action will follow.
- School visits: parents must not, under any circumstances, access social networking accounts whilst assisting staff members. They must also ensure that they do not take photographs/videos on a personal device. If there is evidence to prove that this has happened, then the parent will no longer be used as a helper on subsequent visits. If this is considered a GDPR breach, it will be reported in accordance with our GDPR policy.

Notice and take down policy – should it come to the school's 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 as soon as possible.

Mobile phones/smart devices

- School staff, volunteers, parents and contractors are allowed to bring in personal mobile phones/smart devices for their own use. Staff, volunteers, parents and contractors should use their personal mobile phones/smart devices with caution. The responsible use of personal mobile phones and devices is based on an agreement of trust that; During times when children are on the school premises, phones must be kept on silent, locked and strictly out of sight. Staff, volunteers, parents and contractors may only make and receive calls out of school hours or in an emergency in a private room, not occupied by children.
- Users bringing personal mobile phones/smart devices into school must ensure that there is no inappropriate or illegal content on the device – even if this is not immediately accessible or visible.
- Staff, volunteers, parents and contractors will not use mobile devices to take images or videos of pupils, staff or any area of the school environment. This is strictly prohibited.
- If school staff have a family emergency or similar and are required to keep their personal mobile phone to hand, prior permission must be sought from the Head Teacher.
- Staff, volunteers, parents and contractors will not access the Wi-Fi system using personal mobile devices, unless permission has been given by the Head Teacher.
- Children are permitted to have a mobile phone in school if they are in KS2 and walk to and from school unaccompanied. All mobile phones belonging to children must be switched off and locked away by the class teacher during school hours.

Incidents - Any Online Safety incident is to be brought to the immediate attention of the Online Safety Leaders and the Head Teacher. The Online Safety Leaders and Head Teacher will assist 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, Partney C of E Primary School will have an annual programme of training which is suitable to the audience.

Online Safety for pupils is embedded into the curriculum; whenever IT 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 pupils' learning.

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

The Online Safety Leaders are responsible for recommending a programme of training and awareness for the school year to the Head Teacher 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 Head Teacher for further CPD.

For members of teaching staff there will be updates throughout the year (during staff briefing time) on Online Safety.

REMOTE LEARNING

All remote learning is delivered in line with the school's Remote Learning Policy.

Video Communication (Google Meet)

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Under no circumstances should school video meetings be uploaded to a social media platform (private or

public).
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

- The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.
- Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.
- The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.
- The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.
- The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.
- During the period of remote learning, the school will maintain regular contact with parents to:

-Reinforce the importance of children staying safe online.
-Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
-Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
-Direct parents to useful resources to help them keep their children safe online.
-The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

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

Internet access - You must not intentionally 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 Online Safety incident, reported to the Online Safety Leaders and an incident sheet completed.
Social networking – is allowed in school in accordance with the Online Safety policy only. Staff using social networking for personal use should never undermine or bring into disrepute the school, its staff, parents or children. Under no circumstances should pupils or ex-pupils under the age of 13 be befriended on a social networking website (e.g.: no accepting of 'friend requests' on Facebook). If a child requests the befriending of a staff member, their parents should be informed and the staff member should inform the Head Teacher. In the event that a parent makes contact with a staff member through a social networking website, the staff member must use extreme caution and it is recommended that they provide their school email address as a point of contact for professional purposes. In the event of communicating with a parent or adult associated with a child who attends the school, no comments should be made about pupils, staff or parents. Any statements or status remarks published on personal social media, in any capacity, should not contain any comments about the school, staff, parents or pupils. All views expressed by staff members on social networking websites are their personal views and are in no way endorsed, nor supported, by the school. Staff should always assume that anything posted on social media would be attributed to them as a professional. School employees and volunteers must not identify themselves as associated with the school in any way, unless expressly authorised by the Head Teacher.

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. Under no circumstances should a password be shared with a staff member, pupil or IT technical support staff. If staff feel that a password has been compromised, they should report this to the Head Teacher or Online Safety Leader immediately.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, Chromebook etc.) is encrypted in line with the school Data Protection Policy. On no occasion should data concerning personal information be taken offsite on an unencrypted device. Please contact IT support if you require assistance with this.
Locking Devices – To prevent unauthorised users/pupils accessing staff profiles it is expected that all devices are locked/signed out of when not in use. Devices are not to be left unattended in the school settings when logged in.
Personal Use of School IT – Staff members are not permitted to use IT equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use. School owned devices will not be used by any friends or family members outside of school.

Images and Videos - You should not upload on to any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings). Photographs and videos of children should only be taken on school cameras/iPads. Personal cameras/iPads/mobile phones should not be used under any circumstances for photographs or videos.
Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head Teacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Online Safety Officers if required.
Viruses and other malware - any virus outbreaks are to be reported to the Serco Helpdesk and Education Lincs as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.
Online Safety – is a safeguarding issue and therefore is the responsibility of everyone. As such you will promote positive Online Safety messages in all use of IT whether you are with other members of staff or with students.
iPads – staff are not to log on to the iTunes Store using personal iTunes accounts. No app purchases/downloads should be made without the consent of the Computing Subject Leader or Head Teacher and these will be organised through the Apple Volume Purchase Programme (VPP).

NAME: ……

SIGNATURE : …… DATE: ……

Acceptable Use Policy – Pupils

Partney CofE Primary School Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school IT 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 IT 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 or an adult I trust 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):……

On behalf of …… (pupil)

Date: ……..

Sample Letter to Parents:

Dear Parent/Carer(s),

Use of the Internet in school is a vital part of the education of your child. 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 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 categorises 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 ' enquires@partney.lincs.sch.uk'

We ask that you discuss the attached sheet with your child, explaining the importance of their computer use in school. Please return the slip below and the pupil Policy to school.

Yours sincerely,

Miss S Addison
Head Teacher

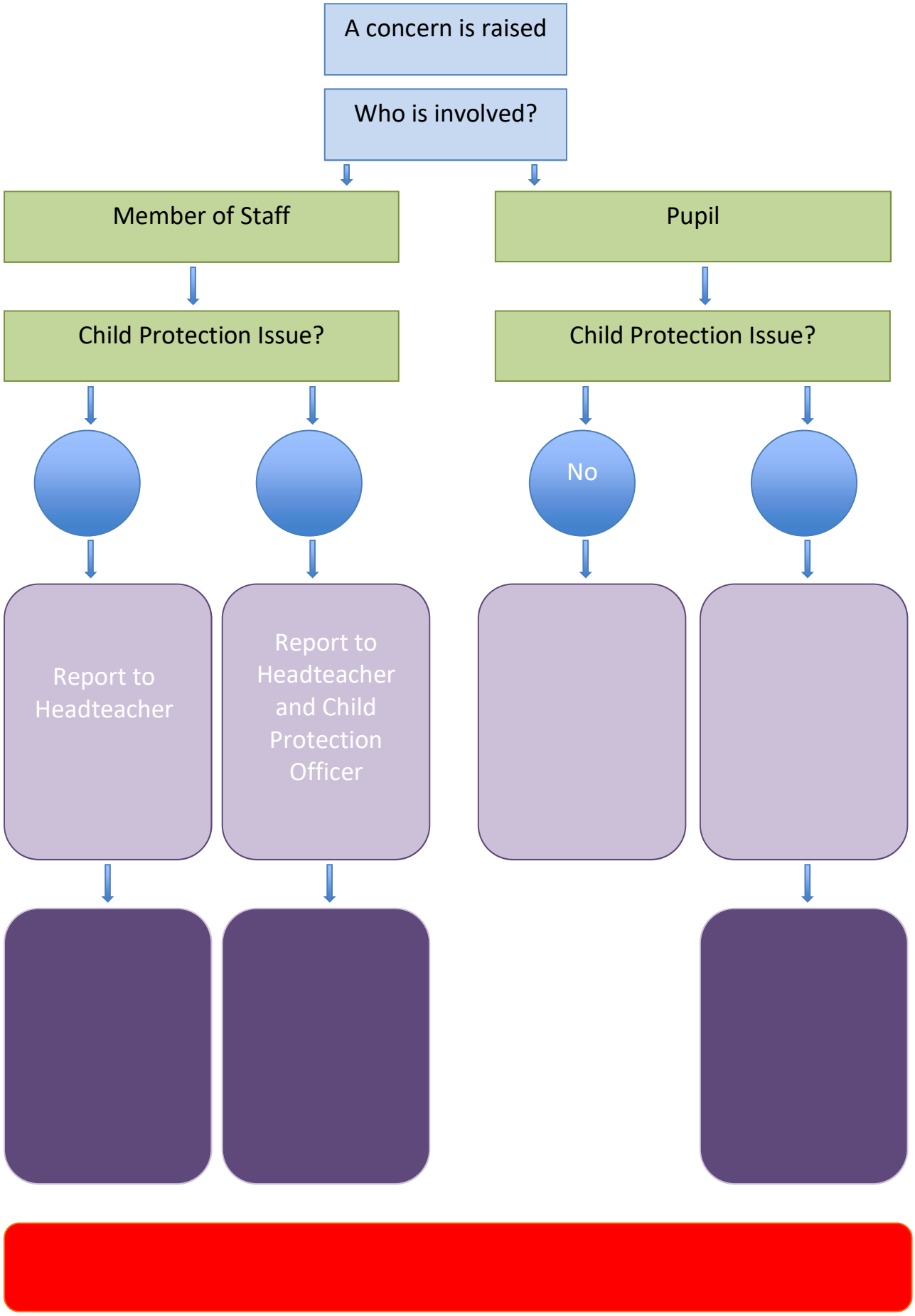
I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion,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

Name of Parent/Carer –

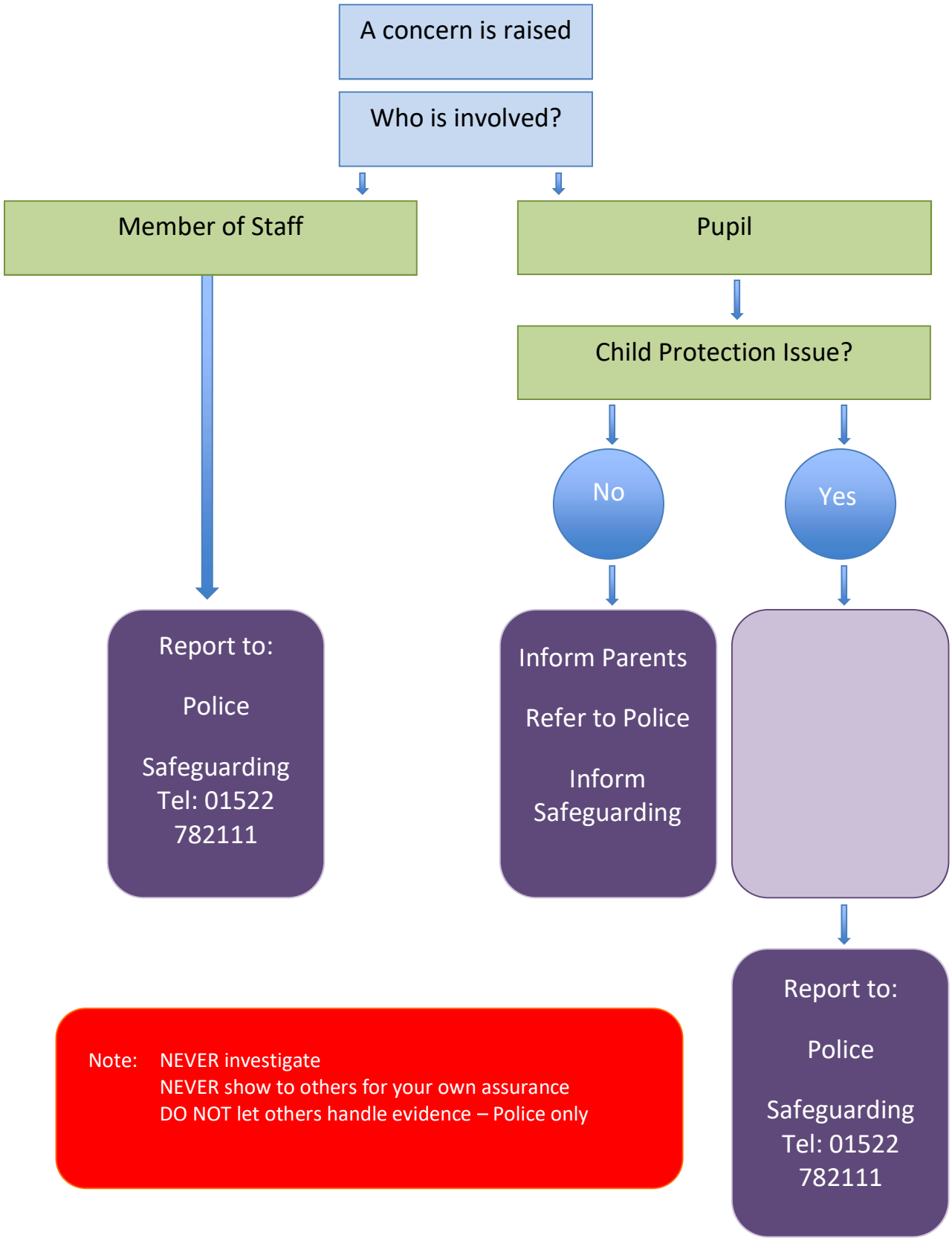
Name of Child –

Signature - Date

INAPPROPRIATE ACTIVITY FLOW CHART



Illegal Activity Flowchart



Risk Assessment

RISK	LIKELIHOOD	IMPACT	SCORE*	ACTIONS
Access to inappropriate content (staff)	1	3	3	Appropriate Internet filtering is in place.
Access to inappropriate content (pupils)	2	3	6	Appropriate Internet filtering is in place, set to a higher level than staff access.
Access to staff files, documentation or filtering level	1	2	2	Pupils should not have access to staff user profiles. The policy states that staff are expected to lock their devices when not in use.
Misuse of copyright material (staff/pupils)	2	2	4	Pupils are taught about copyright as part of the Online Safety element of the Computing curriculum. Staff aware of copyright guidelines.
Loss/theft of personal pupil data	1	3	3	Encryption and security measures to be in place on all IT equipment as necessary.
Misuse/inappropriate activity on pupil devices by pupils	2	3	6	Pupil user accounts are set to pupil level of filtering with certain features/functions disabled and monitored via Meraki Profile. Pupils to be supervised when using devices.
Theft of devices	2	1	2	iPads/Chromebooks are to be locked in a secure cabinet/room and updated regularly with latest software updates. iPads protected with passcodes and GPS location discoverable via built-in software. Chromebooks should be logged out at the end of every use.
Theft of off-site school property (eg: laptops, iPads)	2	3	6	Any off-site device to be encrypted and kept as safe as possible. Staff to ensure necessary due diligence.

*This is the product of the likelihood and impact

1-3 = Low Risk
4-6 = Medium Risk
7-9 = High risk