On Line Safety Policy

Review date	March 2023
Date of next policy review	March 2024

This policy is in line with the Single Equality Policy

Princecroft Primary School
Princecroft Lane
Warminster
Wiltshire
BA12 8NT

Headteacher: Mrs Gemma Pierson

E-mail: admin@princecroft.wilts.sch.uk

Online Safety Policy

This policy should be read and understood in conjunction with the following documents:

- Acceptable Use Agreements (attached as appendices)
- Behaviour Policy
- Anti-bullying Policy
- Safeguarding and Child Protection Policy
- Data Protection and Secure Data Handling Policy
- Remote Learning Policy
- Social Networking Policy (WSCB)
- Staff Code of Conduct
- Guidance for Safer Working Practice for Adults working with Children and Young People (February 2022)
- Keeping Children Safe in Education (DfE)
- Screening, Searching and Confiscation at schools (DfE 09/22)
- Education for a Connected World framework (UK Council for Internet Safety 2020 Edition)
- Teaching online safety in schools (DfE Published January 2023)
- Teachers' Professional Standards (DfE Updated December 2021)
- SWGfL Project Evolve – online safety curriculum programme and resources

Appendices

1 Staff and Volunteer Acceptable Use Agreement

2 Parent/carer Acceptable Use Agreement and permission form

3 Pupil Acceptable Use Agreement, KS1

4 Pupil Acceptable Use Agreement, KS2

5. Online Safety Incident Flow Chart

6. Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart

Contents

1. Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and visitors) who have access to and are users of school's digital systems, both in and out of the school.

The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The 2011 Education Act and The Schools (Specification and Disposal of Articles) Regulations 2012 increased these powers with regard to the searching for and of electronic devices and the deletion of data as did well as the guidance from the DfE entitled Screening, Searching and Confiscation at schools (DfE 09/22)

The school will deal with such incidents within this policy and associated policies as referenced above and will, where known, inform parents of incidents of inappropriate online safety behaviour that takes place out of school.

2. Aims of this policy

The Online School Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication;
- allocates responsibilities for the delivery of the policy;
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours;
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils in the digital world;
- describes how the school will help prepare pupils to be safe and responsible users of online technologies;
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms;
- is supplemented by a series of related acceptable use agreements and flowcharts;
- is made available to staff at induction and through normal communication channels;
- is published on the school website.

3. Policy development, monitoring and review

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)/filtering
- internal monitoring data for network activity
- surveys/questionnaires of pupils, parents and staff

Schedule for the development, monitoring and review of this policy

This online safety policy was approved by the resources committee	March 2023
The implementation of this online safety	The head teacher, governor responsible for online safety and the staff member responsible for online safety
Monitoring will take place	Annually
The resources committee will receive a report on the implementation of the online safety policy	Annually
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, legislation, new threats to online safety or incidents that have taken place. The next anticipated review date	March 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed	Wiltshire Council Safeguarding Officer, LADO, police

4. Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the schools. The acceptable use agreements will be communicated and reinforced through:

- all areas of the school's curriculum and school assemblies
- communication with parents
- staff induction and the staff code of conduct/handbook
- the school website

5. Roles and responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. Whilst this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to the head teacher. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and / or parents online have a responsibility to model safe practice at all times. In addition to the roles and responsibilities outlined below, and to support the implementation of this policy, the school has compiled acceptable use agreements, which provide clear guidance in relevant areas such as conduct, access and use of the school system, removable media, downloading files, sharing information, social networks and devices (both school and personal equipment within and outside school).

Separate agreements have been written for staff, volunteers, pupils and parents/carers who are all expected to read and sign them to acknowledge their responsibilities in this area.

a. Head teacher and senior leaders

The head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding though the day-to-day responsibility for online safety will be delegates to the online safety lead.

The head teacher and another member of the SMT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see Appendix 6: "Responding to incidents of misuse" and relevant disciplinary procedures).

The head teacher is responsible for ensuring that the SMT and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The head teacher and SMT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and to support to those colleagues who take on important monitoring roles.

The SMT will receive termly monitoring reports from the online safety lead at staff meetings.

b. School governors

Mrs Joanna Gutmann is the online safety governor.

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This review will be carried out by the online safety governor who will receive regular updates and information about online safety incidents and monitoring reports form the online safety lead.

The role of the online safety governor will include:

- annual meetings with the online safety lead
- annual monitoring of online safety incident logs
- checking that provision outlined in this online safety policy is taking place as intended
- annual monitoring of filtering/change control logs
- reporting to relevant governors/committee/meeting

c. Online safety lead

The online safety lead is Mrs Beth Foyle, supported by Mrs Jo Chalmers.

The online safety lead will be a member of the SMT with responsibility to:

- work closely on a day-to-day basis with the designated safeguarding lead where these roles are not combined;
- take day-to-day responsibility for online safety, being aware of the potential for serious child protection concerns;
- have a leading role in reviewing the school's online safety policy, procedures and documents;
- promote an awareness and commitment to online safety education/awareness, raising concerns across the school and beyond;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (i.e. misuse – see Appendix 6);
- provide (or identify sources of) training and advice for staff, governors, parents and pupils;
- be aware of external sources of support and guidance in dealing with online safety issues (e.g. local authority, police etc) and liaise with the Local Authority (LA) and other external agencies as relevant;
- liaise with the school's technical support and external providers;
- receive and log online safety incidents to inform practice, policy review and development;
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs;
- attend relevant meetings;
- report regularly to the SMT;

- review emerging technologies for educational benefit and a carry out a risk assessment before use in school is allowed.

d. **Designated safeguarding lead**

The designated safeguarding lead is the head teacher, Mrs Gemma Pierson.

The designated safeguarding lead should be trained in online safety and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal and inappropriate materials
- inappropriate online contact with adults and strangers
- potential or actual incidents of grooming
- cyber-bullying

e. **Curriculum leads**

Curriculum Leads will work with the online safety lead to develop a planned an coordinated online safety programme (e.g. ProjectEVOLVE), with reference to the DfE guidance: ‘Teaching online safety in schools’ (January 2023).

This will be provided through:

- a discrete programme
- PHSE and RHE/SRHE programmes
- a mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant initiatives and opportunities (e.g. Safer Internet Day and Anti-Bullying Week

f. **Teaching staff, support staff and volunteers**

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school online safety policy and practices;
- they understand that online safety is a core part of safeguarding;
- they have read, understood, and signed the staff acceptable use agreement;
- they immediately report any suspected misuse or problem to the online safety lead for investigation/action, in line with the school safeguarding procedures;
- all digital communications with pupils and parents should be on a professional level, professional in tone and content and only carried out using official school systems, emails and technologies that are officially sanctioned by the school;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the online safety policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc, in lessons and other school activities (where allowed) and implement current policies regarding these devices;
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use;
- processes are in place for dealing with any unsuitable material that is found in internet searches;
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource;
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc;

- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

g. Network manager

The school should ensure that the provider of technical support is aware of the school's online safety policy and technical security procedures and ensures:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required online safety technical requirements and any DfE/MAT/LA guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed where necessary;
- that filtering is not the sole responsibility of any single person;
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- the use of the network, internet, learning platforms, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the head teacher for investigation and any subsequent action that might be required;
- monitoring software systems are implemented and updated as agreed in the school's policy.

h. Pupils

Pupils are responsible for using the school's digital technology systems in accordance with the appropriate acceptable use agreement and online safety policy.

They should know and understand the school's rules on the use of mobile devices and digital cameras, including the taking of and use of images and on cyber-bullying

They should know what to do if they, or someone they know feels vulnerable when using online technology.

Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

i Parents/carers

Parents/carers are responsible for using the school's digital technology systems in accordance with the 'Parents/Carers' Acceptable Use Agreement' which they are required to read and sign annually.

The school will take every opportunity to help parents understand the need to use internet and mobile devices in an appropriate way.

Parents/carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents/carers sections of the website/learning platform and online pupil records
- their children's personal devices in the school.

6. Reporting and Responding

It is more than likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that the members of the school community are aware that incidents have been dealt with. Such incidents of misuse will be dealt with through the school's normal behaviour and disciplinary procedures.

There may however be occasions when the school has to respond to reports of illegal misuse and, whilst the school will take all reasonable precautions to ensure online safety for all school users, we recognise that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.

All staff will be made aware of the Appendices 5 and 6: “Online Safety Incident” (Appendix 5) and “Responding to Incidents of misuse” (Appendix 6).

It is important that those reporting an online safety incident have confidence that the report will be treated seriously, dealt with effectively and that there are support strategies in place (e.g. peer support) for those reporting or affected by an online safety incident.

The school will ensure that:

- there are clear reporting routes which are understood and followed by all member of the school community, which are consistent with the school’s safeguarding procedures, as well as the school’s policies on whistleblowing and complaints;
- all members of the school community are aware of the need to report online safety issues/incidents;
- reports will be dealt with as soon as is practically possible;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as relevant.

The designated safeguarding and online safety leads, together with other responsible staff, will have appropriate skills and training to deal with online safety risks.

If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, (see flowchart and user actions chart in Appendix 6) the incident must be escalated through the agreed school safeguarding procedures.

Incidents should be logged using the school’s system.

7. Education and training

a. Education of pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school’s online safety provision and should be effectively threaded through the appropriate pillars in other curriculum areas.

Pupils should be helped to understand the need for the ‘Pupil Acceptable Use Agreement’ and encouraged to adopt safe and responsible use both within and outside school.

The school curriculum is designed and written with reference to the key documents listed below, ensuring breadth and progression in the content to reflect the different and escalating risks that pupils face and covering the principles of online safety:

- Teaching online safety in schools (DfE Published June 2019/updated January 2023)
- Education for a Connected World framework (2020 Edition published by the UK Council for Internet Safety)
- SWGfL Project Evolve – online safety curriculum programme and resources
- Computing Curriculum (DfE 2013)

To ensure the quality of learning and outcomes, the online safety curriculum should be broad, up-to-date, provide opportunities for creative activities and context-relevant with agreed objectives, leading to clear and evidenced outcomes.

Given the rapid changes in this area the school’s provision should be regularly revisited.

Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience. This includes:

- how to use technology safely, responsibly, respectfully and securely;

- where to go for help and support when the have concerns about content or contact on the internet or other online technologies.

The programme will be accessible to pupils of different ages and abilities such as those with additional learning needs or those with English as an additional language.

Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of the information.

As part of the relationship and health education curriculum, pupils are taught about online safety and harms. This includes being taught:

- what positive, healthy and respectful online relationships look like;
- the effects of online actions on others;
- how to recognise and display respectful behaviours online.

Key online safety messages should also be reinforced as part of a planned programme of assemblies and pastoral activities.

Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would require them to access sites normally blocked by the school's filtering system. In such cases, staff can request that filters can be temporarily removed from those sites for the period of study. Any request to do so, should be auditable, with clear reasons for the need and in line with the school's procedures.

Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

b. Contribution of pupils

The school acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised:

- through mechanisms to canvass pupil feedback and opinions;
- by the appointment of digital leaders/anti-bullying ambassadors/peer mentors;
- through pupil representation on the online safety education programme, e.g. peer education, digital leaders, leading lessons for younger pupils and online safety campaigns
- by pupils contributing to the writing and updating of the pupil acceptable use agreement;
- pupils contributing to online safety events with the wider school community, e.g. parents' evenings family learning programmes etc.

c. Staff and volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy.

The online safety lead will receive regular updates through attendance at external training events (e.g. from the South West Grid for Learning (SWGfL)/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations

The online safety lead will provide advice, guidance and training to individuals as required.

Training to all staff will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff, which will be regularly updated and reinforced;

- an audit of the online safety training needs of all staff will be carried out regularly and individual requirements identified through their performance management;
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff;
- training will include explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours;
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements/Code of Conduct;
- Where staff are unsure of their responsibilities or recognise a lack of understanding and therefore a need for further training, they must raise this with their line manager.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings and/or INSET days as required.

c. Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology and online safety, health and safety and safeguarding. This may be offered by:

- attendance at training provided by the LA/MAT, National Governors Association or other relevant organisation (e.g. SWGfL);
- participation in school training and information sessions for staff or parents, which may include attendance at assemblies and lessons.

A higher level of training will be made available to (at least) the online safety governor

d. Parents

- Many parents have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. They may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents through:

- regular communication, awareness raising and engagement on online safety issues, curriculum activities and reporting routes;
- letters, newsletters, the school's web site and learning platform;
- parents' information sessions through awareness workshops and parents' evenings etc, with the involvement of pupils where appropriate;
- high profile events and campaigns e.g. Safer Internet Day;
- reference to the relevant web sites and publications e.g. swgfl.org.uk, www.saferinternet.org.uk, http://www.childnet.com/parents-and-carers

8. Technology

The school is responsible for ensuring that its infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

a. **Filtering**

The service is provided by an externally managed ICT service but the school is still responsible for ensuring that they fully comply with all the school's policies, procedures and acceptable use agreements as well as any local authority and national guidance.

The school's filtering procedures are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.

The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
Access to online content and services is managed for all users.

Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

There are established and effective routes for users to report inappropriate content.

There is a clear process in place to deal with requests for filtering changes

Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Younger pupils will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle.

Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.

Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

b. Monitoring

The school monitors all network use across all its devices and services.

An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored and there is a staff lead responsible for managing the monitoring strategy and processes.

There are effective protocols in place to report abuse/misuse and there is a clear process for prioritising response to alerts that require rapid safeguarding intervention management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance
and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment including:

- physical monitoring (adult supervision in the classroom);
- internet use is logged, regularly monitored and reviewed;
- filtering logs are regularly analysed and breaches are reported to senior leaders;
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention;
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems;
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).

c. Technical security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

There will be regular reviews and audits of the safety and security of school technical systems.

Servers, wireless systems and cabling are securely located and physical access restricted.

There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.

All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Group

All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. Where access needs to be shared, the password should be different to a user's personal one.

All users (adults and pupils) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.

The master account passwords for the school systems are kept in a secure place, e.g. school safe.

Records of pupil usernames and passwords for pupils in key stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user and password requirements for pupils at keys 2 should increase as pupils progress through school.

Emma Dredge (Business Manager) is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.

Appropriate procedures, systems and security measures are in place:

- for users to report any actual/potential technical incident or security breach;
- to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts, which might threaten the security of the school systems and data, which are regularly tested);
- to protect the school's infrastructure and individual workstations with up-to-date endpoint (anti-virus software);
- for the provision of temporary access of 'guests' (trainee/supply teachers and visitors) onto the school's system;
- regarding the personal use of school devices outside of school for all potential users;
- to prevent the authorised sharing of personal data unless safely encrypted or otherwise secured.

d. **Mobile technologies** (including BYOD/BYOT[1])

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of using the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

The school's acceptable use agreements for staff and volunteers, pupils and parents give clear guidance regarding the use of mobile technologies and these are attached as appendices to this policy.

[1] BYOD: bring your own device, BYOT: bring your own technology

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned, multiple users	Authorised device	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	Yes	No
Internet only	Yes	Yes	Yes	No	Yes	Yes

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational, irrespective of whether the device is school owned or personally owned.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education and is consistent with and inter-related to other relevant school polices including but not limited to the safeguarding and child protection policy, the behaviour policy and bullying policy, the staff code of conduct, acceptable use agreements and policies around theft or malicious damage.

Pupils are not permitted to bring any of their own mobile devices into school, including mobile phones and wearable devices. If however they are required in the event of an emergency, mobile phones must be handed in to the class teacher at the start of the day and collected once school has finished.

e. Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks and legal implications associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance.

When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Any images of pupils should only be taken on a school device. The personal device of staff/volunteers must not be used, except in an emergency, when such use must immediately be reported to a member of staff.

Staff/volunteers must be aware of those pupils whose images must not be taken/published and any images of pupils should be deleted from all locations.

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images. This is clearly laid out in the acceptable use agreement for parents. However, there may be occasions where the school requests that parents do not take pictures or videos, but this will only be done if felt absolutely necessary and the school requests that parents are supportive and comply with such requests.

Staff and volunteers are allowed to take digital /video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of those images.

As required by the Data Protection Act, written permission from parents will be obtained before photographs of pupils are taken for use in school or published on the school website/social media. Parents will be informed of the purposes for the use of the images, how they will be stored and for how long, in line the Data Protection and Secure Data Handling Policy.

Photographs published on the school website, or elsewhere, that include pupils will be carefully selected and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Care will be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Pupil's work can only be published with the permission of the pupil and parents.

f Online publishing

The school communicates with parents and the wider community and promotes the school through:

- the school's website
- social media
- online newsletters

The school website is managed by Mrs Jo Chalmers

The school ensures that the Online Safety Policy has been followed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information, thus ensuring that there is least risk to members of the school community, through such publications.

g Data protection

The school has a comprehensive 'Data Protection and Secure Data Handling Policy' written with reference to current legislation and guidance as issued by the Information Commissioner's Office, which clearly details the school's responsibilities and its staff.

The school has appointed an appropriate Data Protection Officer who has an effective understanding of data protection law and is free from any conflict of interest.

9 Social media

a. School use

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:

- ensuring that personal information is not published;

- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues;
- clear reporting guidance, including responsibilities, procedures and sanctions;
- risk assessment, including legal risk;
- guidance for pupils and parents.

School staff should ensure that:

- no reference should be made in social media to pupils, parents or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders;
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff;
- a code of behaviour for users of the accounts (acceptable use agreements);
- systems for reporting and dealing with abuse and misuse;
- understanding of how incidents may be dealt with under school disciplinary procedures.

b. Personal use

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

The school permits staff reasonable and appropriate access to personal social media sites during school hours.

c. Monitoring of social media

As part of active social media engagement, the school may pro-actively monitor the internet for public postings about the school.

The school should effectively respond to social media comments made by others according to a defined policy or process.

When parents express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents should be informed of the school complaints procedure.

d. **Cyberbullying** (including ‘sexting’)

Cyberbullying can be defined as “the use of technologies by an individual or group of people to deliberately and repeatedly upset someone else”[2]

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 young people, school staff and parents understand how cyberbullying is different from other forms of bullying,

[2] Sexual Violence and secual harrassement between children in schools and colleges (DFE 09/21)

how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Behaviour, Anti-Bullying and Safeguarding and Child Protection policies, which include:

- clear procedures set out to investigate incidents or allegations of cyberbullying
- clear procedures in place to support anyone in the school community affected by cyberbullying

All incidents of cyberbullying reported to the school will be recorded.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.

Pupils, staff and parents will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.

Further guidance and advice regarding 'sexting' can also be found through the following links:

- UKCIS 'Advice for schools: Responding to and managing sexting incidents')
- DfE December 2020 - Sharing nudes and semi-nudes: how to respond to an incident (overview)

10. **Outcomes**

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents and is reported to relevant groups.

There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training.

There are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and governors.

Parents are informed of patterns of online safety incidents as part of the school's online safety awareness raising.

Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.

The evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

11. **Handling of complaints**

Parents and pupils will need to work in partnership with the school to resolve issues.

Where complaints do not involve acts which are clearly illegal (e.g. accessing child abuse images or distributing racist material) they should be dealt with through the school's normal complaints procedures as outlined in the school's complaints policy.

Complaints regarding Illegal activity would be dealt with in line with the school's safeguarding and disciplinary procedures and where required, would involve contact with the police and could lead to criminal prosecution, as could clear cases of cyberbullying.

As detailed above, there are clear procedures in place to deal with concerns around cyberbullying and such incidences should be brought to the attention of the school as early as possible.

Any complaint about staff misuse must be referred to the head teacher.

Any complaint about the head teacher should be referred to the chair of governors**.**

Where any member of the school community has breached the terms of their respective acceptable use agreement, the school reserves the right to restrict their access to the school's internet.

Appendix 1

Acceptable Use Agreement

Staff and Volunteers

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure that:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. Where it is necessary to share access, login details will be different to the personal ones normally used by staff. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images
- . Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will abide by copyright law in my use of published material

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to governors/trustees and/or the local authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed: ....

Name: ....

Date: ....

Appendix 2

Acceptable Use Agreement

Parent/carer Permission Form

Provided in digital format for signature

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

———

As the parent/carer of the above pupils, I give permission for my son/daughter to have access to the digital technologies at school.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Digital signature required (parent/carer name, pupil name, class)

This form will be available to staff at Princecroft School, it will be stored electronically whilst my child attends the school.

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. The school will also ensure that when images are published children cannot be identified by the use of their full names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Images may be published on platforms such as Twitter, Facebook, local press and on the school website. Parents/carers can ask for images to be deleted by emailing the school office.

This form will be available to staff at Princecroft School, it will be stored electronically whilst your child attends the school.

Digital response to questions below required.

As the parent/carer of the above pupil, I agree to the school taking digital/video images of my child. YES / NO

I agree to these images being used:

- to support learning activities. YES / NO
- in publicity that reasonably celebrates success and promotes the work of the school. YES / NO

I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images YES / NO

Use of Cloud Systems Permission Form

The school uses Oakwood Technology for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil as part of the school's online presence in Google Classroom, SeeSaw, Scratch, Tinkercad

Using these services will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Digital response to consent below:
SeeSaw (whole school
Google Classroom (KS2, years 3-6
Scratch (KS2, years 3-6
Tinkercad (year 6)

Link to digital form:
https://forms.office.com/pages/responsepage.aspx?id=capkmaJDfkCr34E1a8HdDdENhqk4vUFLr7dpqAp5GoJUNkNTQlI4R0ZYUFRUOExRSVFVTFVaUzJZSS4u

Appendix 3

Acceptable Use Agreement

Key Stage One

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use apps, programs or websites that a teacher or suitable adult has told, or allowed me, to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / iPad, I might have to see Mrs Pierson or my parent/ carer may be called.

Signed (child): ....

Date: ....

Appendix 4

Acceptable Use Agreement

Key Stage Two

For my own personal safety:

- I understand that the school may monitor my use of the devices and internet.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

When using the internet for research or recreation, I recognise that:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I will look after the devices I use:

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I have been given permission to do so by an adult in class.

- I will not install or attempt to install any programs/ apps.
- I will not try to change any laptop or iPad settings.
- I will only use websites or apps with permission and at the time I am told to use it- I will not change to another app.

I understand that I am responsible for my actions:

- I understand that if I fail to follow this Acceptable Use Agreement, I will be subject to consequences. This may include: not being able to use the devices on another occasion, loss of playtime, being sent to Mrs Pierson or my parents may be contacted.

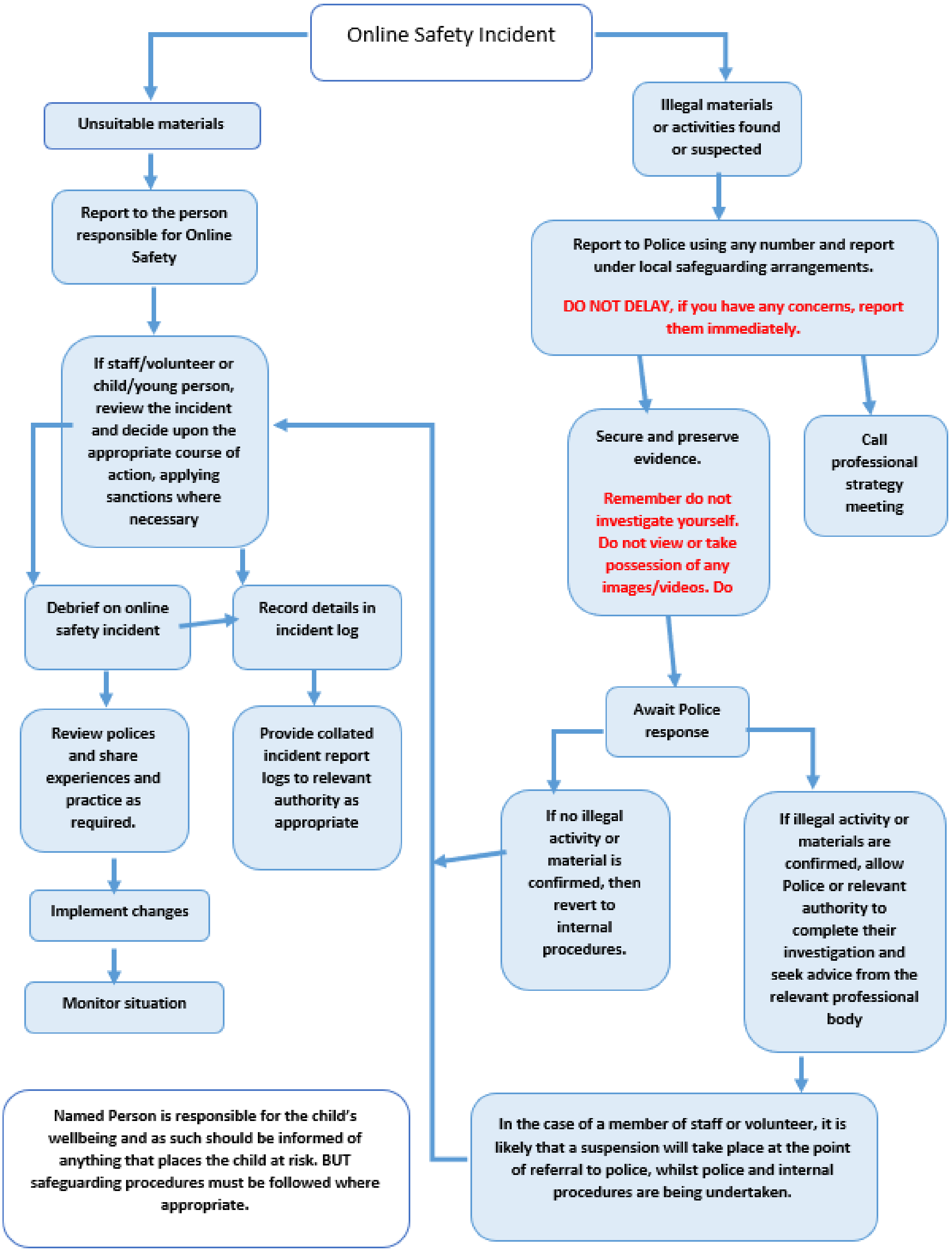
Signed (child): ....

Date: ....

Appendix 5

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

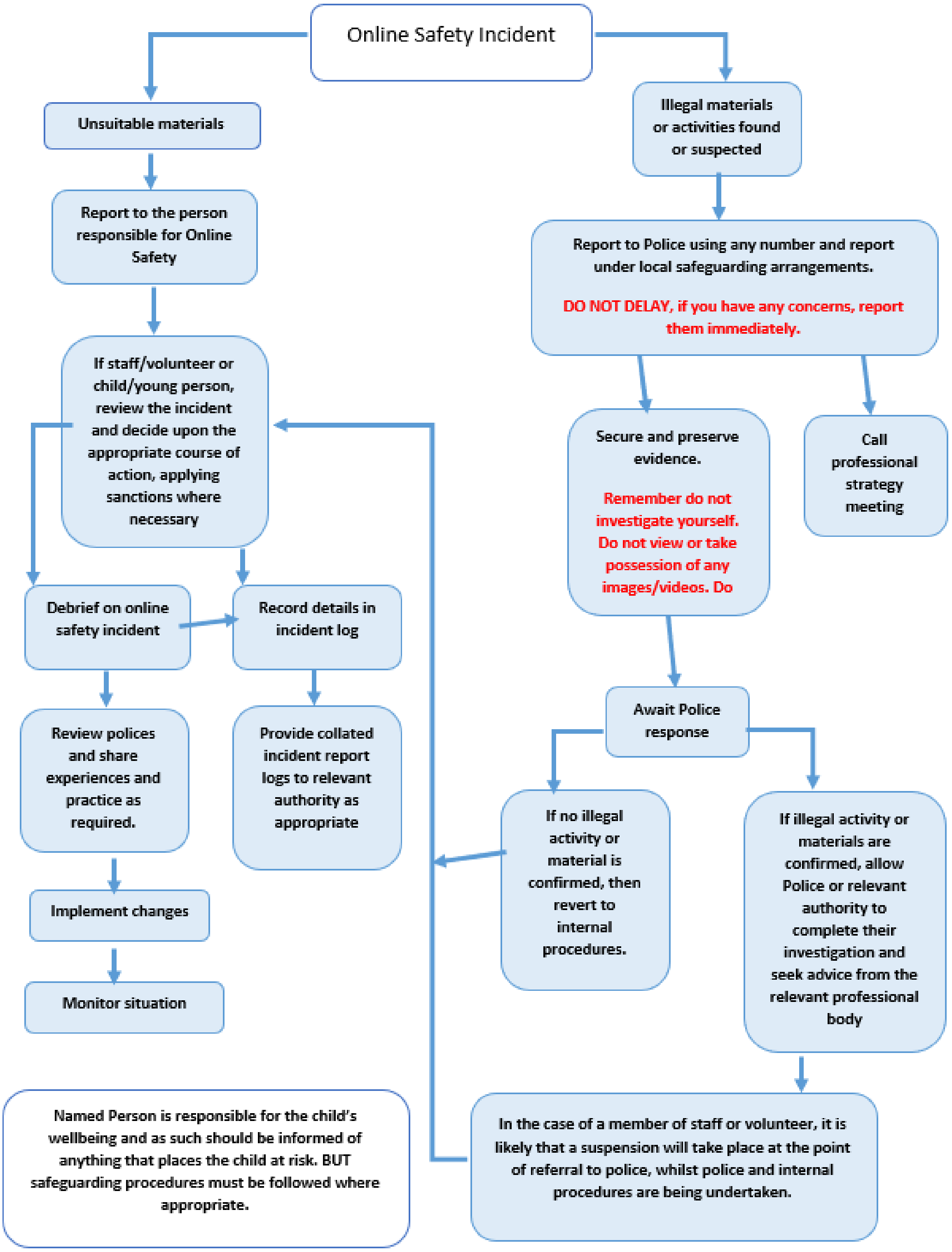
If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix 5

Responding to incidents of misuse



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.