EDGEBOROUGH SCHOOL

E-Safety Policy

(including EYFS and Boarding)

UPDATE LOG

DATE	CHANGE/NOTES	By Whom
09/09/2021	Major policy review	EB and TB

Contents

Development/Monitoring/Review of this Policy **4**

Schedule for Development/Monitoring/Review **4**

Scope of the Policy **5**

Roles and Responsibilities **5**

Governors/Board of Directors 5

Headteacher and Senior Leaders 6

Online Safety Lead (DSL) 6

Network Manager/Head of IT 6

All Staff including Activity Providers 7

Designated Safeguarding Lead 7

Online Safety Group 8

Students/Pupils: 8

Parents/carers 8

Policy Statements **9**

Education – Pupils 9

Education – Parents/carers 10

Education – The Wider Community 10

Education & Training – Staff/Volunteers 10

Training – Governors 11

Technical – infrastructure/equipment, filtering and monitoring **11**

Mobile Technologies (including BYOD) **12**

Use of digital and video images **13**

Data Protection **13**

Communications **14**

Social Media - Protecting Professional Identity **14**

Dealing with unsuitable/inappropriate activities **14**

Responding to incidents of misuse **17**

Illegal Incidents **17**

Other Incidents **18**

School actions & sanctions **19**

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of: Ellie Buckey (Deputy Head Pastoral and DSL), Tim Barette (Head of IT), Lee Barnard (Network Manager) and Jayne Symons (Head of Pre-Prep). The policy is then checked by other members of ELT and governors. It is made available to the rest of the school community via our website. We welcome input from other staff and parents as we are constantly reviewing online safety and aiming to improve it.

This policy should be read in conjunction with:

- The taking, storing and using images of children policy.
- The IT acceptable use policy.
- The data protection policy.
- The Safeguarding policy.
- The Staff Code of Conduct.
- The Behaviour Policy.

Schedule for Development/Monitoring/Review

This E-safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*5th October 2021*
The implementation of this E-safety policy will be monitored by the:	*Executive Leadership Team*
The E-safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually*
The Governing Body will receive a report on the implementation of the E-safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*

The school will monitor the impact of the policy using:

- Logs of reported incidents.

- Monitoring logs of internet activity via our filtering service 'Smoothwall'.
- Surveys/questionnaires of students/pupils, parents/carers and staff.

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, activity providers) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers 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 online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy, Safeguarding Policy and Policy for searching pupils' possessions.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors/Board of Directors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, as part of the Safeguarding Governor role. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator (who is also the DSL).
- Attendance at Online Safety Group meetings.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting to relevant Governors/Board/Committee/meeting.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the DSL.
- The Headteacher and (at least) another member of the Senior Leadership Team 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.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead (DSL) 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 Headteacher and Senior Leaders 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 also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive monitoring reports from the Online Safety Group.

Online Safety Lead (DSL)

- Leads the Online Safety Group.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meetings of Governors.

Network Manager/Head of IT

Those with technical responsibilities are responsible for ensuring:

- 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 that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

- That 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.
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as necessary.

All Staff including Activity Providers

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the staff acceptable use policy/agreement (AUP) on joining the school. Reference is made to online safety in the Staff Code of Conduct which is reviewed annually and signed for by staff.
- They report any suspected misuse or problem to the Headteacher/ /DSL for investigation/action/sanction.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the acceptable use policies and any relevant parts of this E-safety Policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils are 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.

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- online-bullying.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Lead (DSL) with:

- the production/review/monitoring of the school online safety policy/documents.
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- Monitoring network/internet/filtering/incident logs.
- Consulting stakeholders – including parents/carers and the pupils about the online safety provision.
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- 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.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and 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' sections of the website/Learning Platform and on-line student/pupil records;
- their children's personal devices in the school or devices the children have been leant by the school.

Policy Statements

Education – 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/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PHSE lessons and is regularly revisited. The school follows the Education for a Connected World Framework in order to plan the Online Safety Curriculum.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils should be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- 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.
- Pupils are helped to understand the need for the pupil acceptable use agreement and required to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/carers

Many parents and carers have only 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/regulation of the children's online behaviours. Parents 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 and carers through:

- curriculum activities.
- Letters, newsletters, web site.
- Parents/carers evenings/sessions.
- High profile events/campaigns e.g. Safer Internet Day.
- Providing further guidance and resources.

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Sharing their online safety expertise/good practice with other local schools.

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Group will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.

- This E-safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Group will provide advice/guidance/training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- 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/academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager/Head of IT who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering.

- The School regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- In the event of a technical incident/security breach, pupils would report to their member of teaching staff and staff members would report to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.
- A separate Acceptable Use of IT policy is in place for pupils in Years 6-8 who are issued with school devices that may be used out of school.
- A separate Acceptable Use of IT policy is in place for all school staff and other adults working in the school.

Mobile Technologies (including BYOD)

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*[2]	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*

[1] Authorised device – purchased by the school for use by pupils in Years 6-8.

[2] The school permits children on the LEAP register to bring in a personal device if appropriate to support learning. This is covered by the BYOD policy.

Use of 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/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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 will also ensure:

When using digital images, staff 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.

- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press.
- 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.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should 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.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully 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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

For further information, please see our Data Protection Policy.

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Please see the separate Social Media Policy.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	

	Promotion of extremism or terrorism				X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices. • Creating or propagating computer viruses or other harmful files. • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords). • Disable/Impair/Disrupt network functionality through the use of computers/devices.					X
• Using penetration testing equipment (without relevant permission).					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	

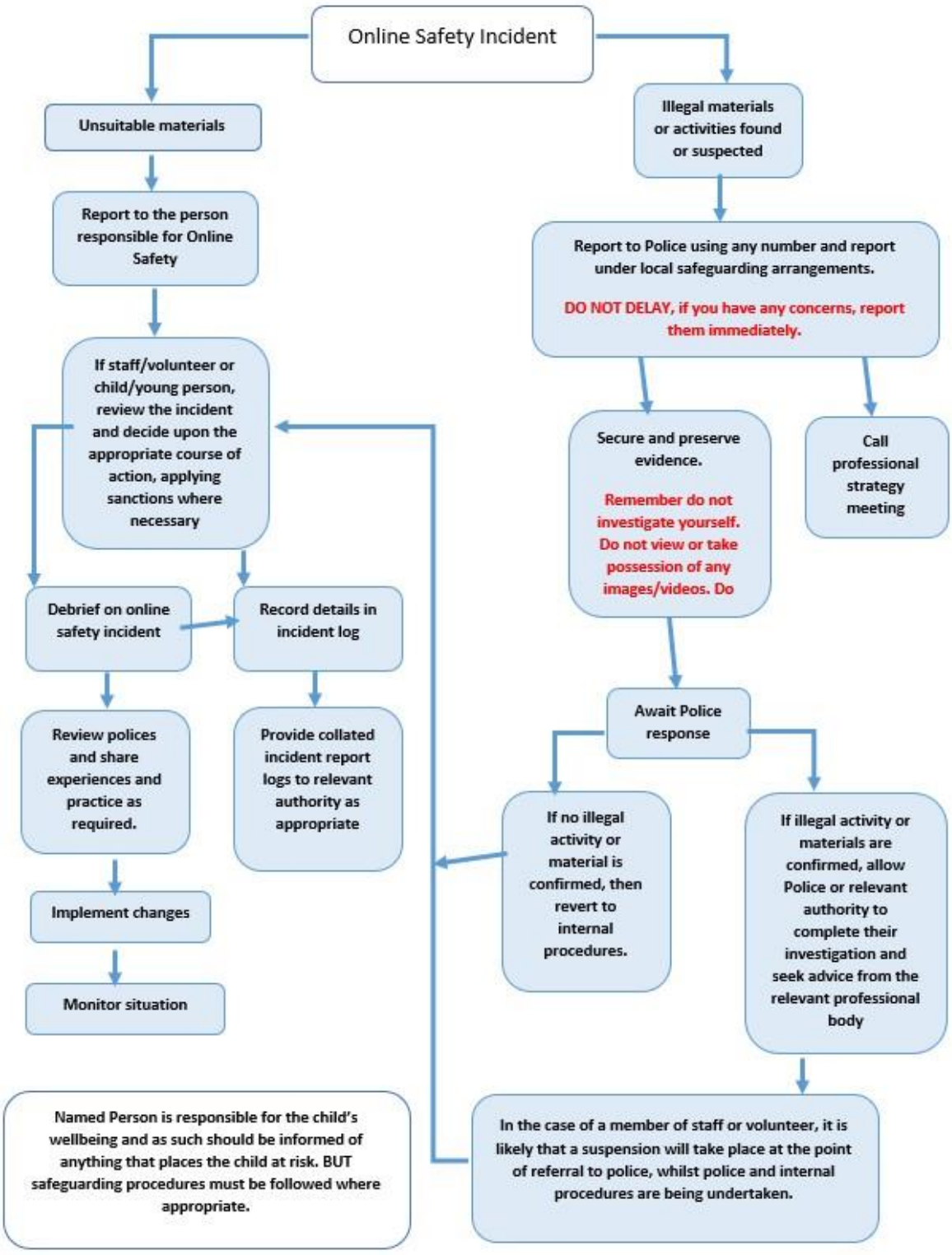
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce		X			
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when

infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures ○ Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour ○ the sending of obscene materials to a child ○ adult material which potentially breaches the Obscene Publications Act ○ criminally racist material ○ promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above) ○ other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more 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 members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows. These are outlined in the relevant Acceptable Use Policies for staff and students.