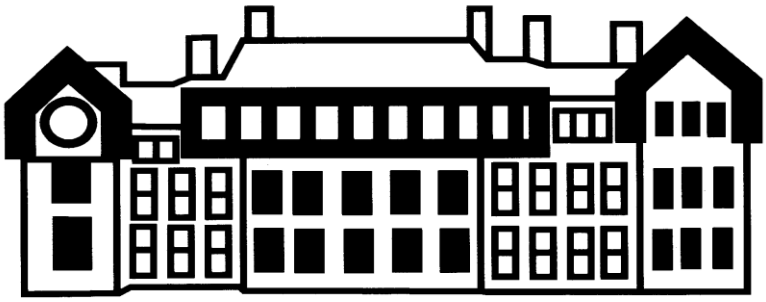
GORDON



SCHOOL

E-Safety Policy

Ratification date: November 2017

Review date: November 2020

Signed _____ Headteacher

Signed _____ Chair of Governors

E-Safety Policy

Includes: Acceptable Use Agreements
See also: Safeguarding & Child Protection Policy
Photography & Recording of Images Policy
Anti-Bullying Policy
Behaviour and Discipline Policy
Staff Handbook

1, Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents, carers, visitors and community users) who have access to, and are users of, school computing 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to members of the school community. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered in the school's published *Behaviour & Disciplne Policy*.

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

2, Aims

This policy aims to explain how children, parents and staff can be a part of these safeguarding procedures. It also details how children are educated to be safe and responsible users of technology, capable of making good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children and adults from potential and known risks.

This policy has four aims:

- to emphasise the need to educate members of our community including but not exclusively: staff, children and parents about the positive and negative aspects associated with using technologies both within and outside school;
- to provide safeguards and agreement for acceptable use to guide all users, whether staff, pupil or visitor, in their online experiences;
- to ensure clarity regarding the procedures for dealing with the misuse of any technologies both within and beyond the school; and
- to develop links with parents and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

3, Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the *E-Safety Policy* and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has the role of Child Protection / Safeguarding Governor and this role also covers E-Safety. The role of this Governor will include:

- regular meetings with the member of staff responsible for e-safety (the Computing subject leader);
- regular monitoring of e-safety incident logs;
- regular monitoring of filtering / change control logs;
- reporting to the Governors Body;
- challenging the school on its use of firewalls, anti-virus and anti-spyware software.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of all members of the school community.
- The Headteacher and (at least) one other member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Computing Subject Leader receives suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will inform the Governors at least annually about the progress of, or any updates to, the e-safety curriculum and ensure Governors know how this relates to safeguarding.

The Computing Subject Leader:

- takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with the Local Authority when necessary;
- liaises with school technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- meets with the e-safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant meetings with Governors;
- reports regularly to the Headteacher;
- ensures that the *Acceptable Use Agreements* (AUA) are reviewed annually;

- liaises with subject leaders so that policies are up-to-date and take account of any emerging issues and technologies;
- ensures that staff can check for viruses on school equipment and memory sticks or other transferable data files to minimise issues of virus transfer;
- ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- keeps up-to-date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- ensures that the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher.

Teaching and Support Staff:

The staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school *E-Safety Policy* and practices;
- they have read, understood and signed the *Acceptable Use Agreement* (AUA);
- they report any suspected misuse or problem to the Headteacher for investigation, action or sanction;
- all digital communications with parents and carers should be on a professional level and only carried out using official school systems;
- there is no digital communication with pupils in any form whatsoever unless it takes place within a lesson;
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the *E-Safety Policy* and the *Acceptable Use Agreements*;
- 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 (including homework) where internet use is pre-planned, 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.

Child Protection/ Safeguarding Designated Teacher:

The Child Protection/Safeguarding Designated Teacher should be trained in e-safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

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

- cyber-bullying.

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 and use of images and on cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's *E-Safety Policy* covers their actions out of school, if related to their membership of the school.

Parents:

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through information evenings, newsletters, letters, workshops and the school website. Information about national and local e-safety campaigns or initiatives will be shared. Parents will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to the school's website.

Community Users:

Community users (visitors, volunteers, etc) who access school systems as part of the wider school provision will be expected to sign an *Acceptable Use Agreement* before being provided with access to school systems.

4, E-Safety Education

Technology brings many advantages and benefits with it but there are also negative aspects. Education around these issues and how to deal with them is vital.

Education for Pupils

The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- a planned e-safety curriculum should be provided;

- key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;
- pupils should be taught in all lessons to be critically aware of the materials 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 helped to understand the need for the pupil *Acceptable Use Agreement and* encouraged 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. 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.
- Where pupils are allowed to freely search the internet, staff should be 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 and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 for Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Education for Parents

Many parents have only a limited understanding of e-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 on-line behaviour. 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 through:

- curriculum activities;
- letters, newsletters and the school's website;
- Open Evenings;
- high profile events or campaigns;
- reference to the relevant web sites and publications.

Education for Staff and Volunteers

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

- a programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school *E-Safety Policy* and *Acceptable Use Agreements*.
- The E-Safety Leader will receive regular updates through attendance at external training events (e.g. from the Local Authority) 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 / phase meetings / INSET days.
- The E-Safety Leader (or other nominated person) will provide advice / guidance / training to individuals as required.

Education for Governors

Governors should take part in e-safety training, with particular importance for those who are involved in technology, e-safety, health and safety or child protection. This may be offered in a number of ways:

- attendance at training provided by the Local Authority, National Governors Association or other relevant organisations;
- participation in school training or information sessions for staff.

5, Technical Security

The school will be responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that 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 e-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 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;
- the Headteacher is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations. This responsibility is delegated to the Computer Subject Leader and School Business Manager;
- internet access is filtered for all users;
- school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the *Acceptable Use Agreement.*

- an appropriate system is in place (see appendix) for users to report any actual or potential technical incident or security breach to the relevant person, as agreed;
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, 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 workstations are protected by up to date virus software;
- an agreement is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers and other visitors) onto the school systems.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6, 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 and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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:

- When using digital images, staff should 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.
- 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 is 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 or video images.
- Staff are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. Volunteers, e.g. student teachers, need to seek permission from the Headteacher.
- Care should be taken when taking digital or 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 school 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, unless permission is given by parents.
- Written permission from parents will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents.

7, Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

The school must ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing";
- it has a *Data Protection Policy;*
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs);
- risk assessments are carried out;
- it has clear and understood arrangements for the security, storage and transfer of personal data;
- data subjects have rights of access and there are clear procedures for this to be obtained;
- there are clear and understood policies and routines for the deletion and disposal of data;
- there is a policy for reporting, logging, managing and recovering from information risk incidents;
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;

- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- transfer data using encryption and secure password protected devices.

8, Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices eg tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network			✓					✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓

Use of social media			✓					✓
Use of blogs (Edmodo with appropriate permissions signed by parents/carers)	✓				✓			

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 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 parents (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class or group email addresses may be used in Key Stage 1, while pupils in Key Stage 2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-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.

9, Social Media – Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly, for acts carried out by their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of a “protected characteristic” or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- clear reporting guidance, including responsibilities, procedures and sanctions.
- risk assessment, including legal risk.

School staff and governors should ensure that:

- no reference should be made in social media to pupils, parents, families 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 or local authority;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the E-Safety Leader to ensure compliance with the relevant school policies.

10, Unsuitable and Inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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	

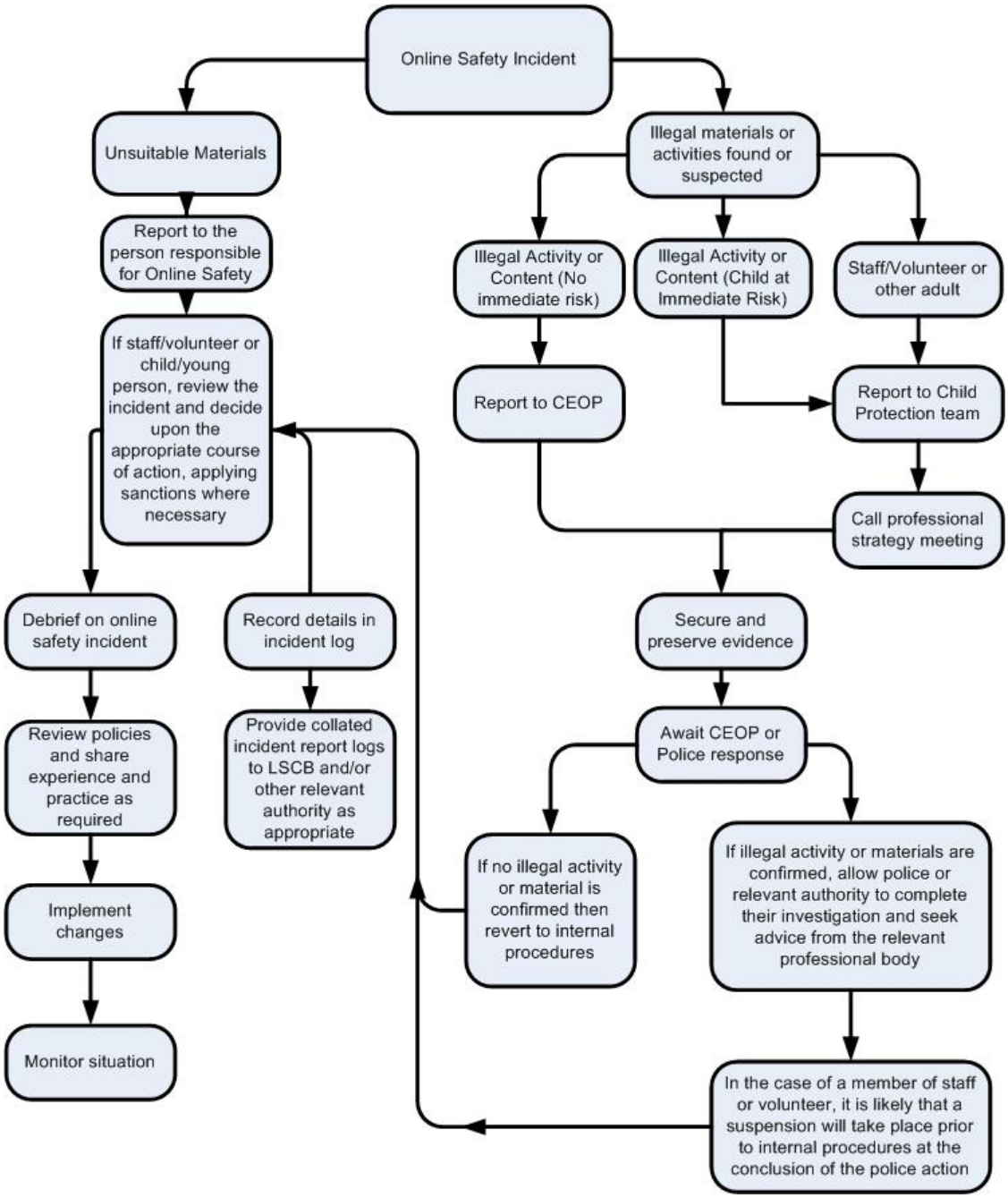
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					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. You Tube			X			

11, 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 (see “User Actions” above).

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:

- There should be 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 there has been a full investigation 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;
- 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;
- other criminal conduct, activity or materials;

Isolate the computer in question. 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and 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:

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security, etc.	Inform parents / carers	Removal of network/ internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X

Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering, etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X					X

Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

12 Monitoring and Review

It is the responsibility of the Governing Body to monitor the safety of pupils and they will receive an annual report from the Headteacher. The Governing Body also has the responsibility for this policy, and for seeing that it is carried out.

This policy will be reviewed every three years, or sooner if deemed necessary by the Governing Body.

Acceptable Use Agreement for Staff, Governors and Visitors

School networked resources, including online or cloud based resources, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or Local Authority you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or Local Authority into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility

- Users are responsible for their behaviour and communications. Staff, Governors, volunteers and visitors will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the E-Safety Leader.

Acceptable Use

- Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.
- Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos and code of conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or Royal Borough of Greenwich) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to pupils.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and contact the E-Safety Leader.
9	I will ensure that I log off after my network session has finished.

10	If I find an unattended machine logged on under other users username I will not continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the Senior Leadership Team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches or unsuitable websites to the E-Safety Leader.
15	I will not use "USB drives", portable hard-drives, mass storage devices or personal laptops on the network without having them "approved" by the school and checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through *friends* and *friends of friends*. This applies especially to those connected with my professional duties, such a school parents and their children.
19	I will ensure that any private social networking sites or blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
20	I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on the school's MIS.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent or received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

Additional guidelines
Staff must comply with the *Acceptable Use Agreement* of any other networks that they access.

Services
There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Network Security
Users are expected to inform the E-Safety Leader immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the E-Safety Leader. Users identified as a security risk will be denied access to the network.

Media Publications
Written permission from parents must be obtained before photographs of or named photographs of students are published. Also, examples of pupils' work must only be published (e.g. photographs, videos, TV presentations, web pages etc.) if parental consent has been given.

Staff / Governor / Volunteer / Visitor *Acceptable Use Agreement* Form

As a school user of the network resources, I agree to follow the school rules (set out above) on its use.

- I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the E-Safety Leader
- I agree to report any misuse of the network to the E-Safety Leader. I also agree to report any websites that are available on the school Internet that contain inappropriate material to the E-Safety Leader.
- I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the E-Safety Leader.

- If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Name: _____

Signature: _____

Date: _ _ /_ _ /_ _ _ _

Pupil *Acceptable Use Agreement*

All pupils must follow the rules in this agreement when using school computers, or when logged into internet sites using a school login.

Pupils that do not follow these rules may find:

- they are not allowed to use the computers,
- they can only use the computers if they are more closely watched.

Computer Rules	
1	I will only use polite language when using the computers.
2	I must not write anything that might: upset someone or give the school a bad name.
3	I know that my teacher will regularly check what I have done on the school computers.
4	I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5	I must not tell anyone my name, where I live, or my telephone number - over the Internet.
6	I must not tell my username and passwords to anyone else but my parents or carers.
7	I must never use other people's usernames and passwords or computers left logged in by them.
8	If I think someone has learned my password then I will tell my teacher.
9	I must log off after I have finished with my computer.
10	I know that e-mail is not guaranteed to be private. I must not send unnamed e-mails.
11	I must not use the computers in any way that stops other people using them.
12	I will report any websites that make me feel uncomfortable to my teacher or another adult in school.
13	I will tell my teacher or another adult in school straight away if I am sent any messages that make me feel uncomfortable.
14	I will not try to damage any equipment or the work of another person on a computer.
15	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

Unacceptable Use

Examples of unacceptable use include, but are not limited to:

- using a computer with another person's username and password;
- creating or sending on the internet any messages that might upset other people;
- looking at, or changing work that belongs to other people;
- wasting time or resources on school computers.

Pupil *Acceptable User Agreement* Form

- I agree to follow the school rules when using the school computers.
- I will use the network in a sensible way and follow all the rules explained by my teacher.

- I agree to report anyone not using the computers sensibly to my teacher.
- I agree to tell my teacher or another member of staff if I see any websites that make me feel unhappy or uncomfortable.
- If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Pupil Name: _____

I realise that any pupil under reasonable suspicion of not following these rules when using the computers may have their use stopped, more closely monitored or past use investigated.

Parent/Carer's Name: _____

Parent/Carer's Signature: _____

Date: _ _ / _ _ / _ _ _ _