



Dorothy Barley Junior Academy

Online Safety

Policy and Audit

September 2019

LBBD ICT Team, Children's Services

Based on documents from:
South West Grid for Learning
London Grid for Learning
Kent County Council

Online Safety Policy Review

The online safety policy relates to other policies including those for Computing and ICT, bullying, child protection and data protection.

Policy review date:	September 2019
Policy reviewed by:	SLT
Next policy review date (at least annually):	September 2020

Contents

Introduction and Overview:

- Purpose of the Policy
- Scope of the Policy
- Online Safety Audit

Roles and Responsibilities:

- Online Safety Coordinator / Designated Child Protection Lead
- Governors / Online Safety Governor
- Computing / ICT Subject Leader
- Network Manager / Technical staff / Computing Subject Leader
- Data and Information Manager
- Teaching and Support Staff
- Pupils
- Parents / Carers
- Community Users

Education and Training:

- Pupils
- Staff and Governors
- Parents / Carers

Managing the Infrastructure, Equipment and Content:

- Access, Security and Filtering
- Password Policy
- Personal Devices
- Data Protection
- Use of Digital and Video Images
- Email and Communications
- Social Media – Staff (Protecting Professional Identity)
- Social Media – Pupils

Incident Management:

- Responding to Incidents
- Responding to Incidents – Flow Chart

Appendix 1 – Online Safety in Computing Programme of Study

Appendix 2 – Handling a Sexting Incident

Introduction and Overview

Purpose of the Policy

Schools must have an online safety policy covering the safe use of internet and electronic communications technologies such as mobile phones and internet connected devices. The policy will highlight the need to educate children, young people and their families about both the benefits and risks of using technologies both in and away from the school context. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

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 cyberbullying, 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.

Schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. There are additional duties under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.

The school's Online Safety Policy will operate in conjunction with other policies including Behaviour, Bullying, Curriculum, Data Protection, Safeguarding, Information Security and any Home-School Agreements.

Scope of the Policy

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

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be available via the school office / network / website
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Online Safety Audit (2019-20)

This audit is completed by the member of the Senior Leadership Team (SLT) responsible for the online safety policy. Staff who contribute to the audit include the Child Protection coordinator, Data Protection / GDPR Officer, Data Security Officer, SENCO, Online Safety coordinator, ICT Subject Leader and Headteacher.

Date of latest update of the online safety policy (at least annual):	
The school online safety policy was agreed by governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The online safety coordinator is:	
The member of the Senior Leadership Team responsible for online safety is:	
The member of the Governing Body responsible for online safety is:	
The Child Protection coordinator is:	
The Data Protection Officer is:	
Has online safety training been provided for all staff?	Y/N
Has online safety guidance been provided for all pupils?	Y/N
Are online safety guidance materials available for parents?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Have online safety materials from CEOP and other agencies been considered?	Y/N
Have all staff (teaching and non-teaching) signed the Staff Acceptable Use Agreement?	Y/N
Have all pupils signed the Pupil Acceptable Use Agreement?	Y/N
Have all parents/carers signed an Online Safety home / school agreement form?	Y/N
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Is personal data collected, stored and used according to the principles of the General Data Protection Regulation?	Y/N
Is Internet access provided by an approved educational internet service provider (e.g. RM)?	Y/N
Has filtering on internet-based devices been appropriately applied?	Y/N

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school (in some cases the roles described may be combined):

Headteacher

- To take overall responsibility for the safety (including online safety) of members of the school community
- To take overall responsibility for data management and information security ensuring the school follows best practice in information handling
- To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their safeguarding and online safety roles
- To be aware of procedures to be followed in the event of a serious online safety incident
- To receive regular monitoring reports from the Online Safety Coordinator / Officer

Senior Leadership and Inclusion Team

- To take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
- To promote an awareness and commitment to online safety throughout the school community
- To ensure that online safety education is embedded within the curriculum
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- To ensure that online safety incidents are logged as safeguarding incidents
- Is regularly updated in online safety issues and legislation, and is aware of the potential for serious child protection issues
- To facilitate training and advice for all staff
- To liaise with the Local Authority and relevant agencies
- To communicate regularly with the Local Authority to discuss current issues, review incident logs and filtering / change control logs

Governors

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To approve the Online Safety Policy and review the effectiveness of the policy
- To support the school in encouraging parents and the wider community to become engaged in online safety activities
- The role of the Online Safety Governor will include regular review with the Online Safety Coordinator (the Governor role may be combined with that of the Child Protection / Safeguarding Governor)

ICT Subject Leader

- To oversee the delivery of the online safety element of the Computing curriculum

ICT Technician Link

- To ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack, e.g. by keeping virus protection up to date
- To ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- To report any online safety related issues that come to their attention to the Online Safety Coordinator
- To ensure the school's policy on web filtering is applied and updated on a regular basis
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To keep up to date with the school's online safety and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- To regularly monitor the use of school technology and online platforms and that any misuse / attempted misuse is reported to the Online Safety Coordinator / Headteacher
- To ensure that the data they manage is accurate and up-to-date
- To ensure best practice in information management, i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.

Teaching and Support Staff

- To ensure they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
- To report any suspected misuse or problem to the Online Safety Coordinator / Headteacher
- To ensure that any digital communications with pupils / parents / carers should be on a professional level and only through school based systems, e.g. not on personal email, mobile phones etc.
- To embed online safety in the curriculum
- To ensure that pupils understand and follow the Online Safety Policy and Pupil Acceptable Use Agreement
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- To ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To 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
- To model safe, responsible and professional behaviours in their own use of technology

Pupils

- To read, understand, sign and adhere to the Pupil Acceptable Use Agreement annually
- To understand the importance of reporting abuse, misuse or access to inappropriate materials, and how to do so
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe behaviours and 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
- To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To know, understand and adhere to the school policy on the use of mobile devices and digital cameras, including the taking / use of images and cyberbullying

Parents / Carers

- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement, including the use of photographs and video images and pupils' use of the internet
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To consult with the school if they have any concerns about their children's use of technology
- To model safe, responsible and positive behaviours in their own use of technology

Community Users

- Any external individual / organisation will sign an Acceptable Use Agreement prior to using technology or the internet within school
- To support the school in promoting online safety
- To model safe, responsible and positive behaviours in their own use of technology

Education and Training

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 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 message across the curriculum.

See appendix 1 for the online safety statements from the Computing Curriculum programme of study.

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 should be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should sign and follow the guidance outlined in the Acceptable Use Agreement
- Pupils should be taught and encouraged to adopt safe and responsible use of technology both within and outside school, including appropriate online behaviour and keeping personal information private
- Pupils should be taught in lessons to be critically aware of the materials / content they access online 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
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices, e.g. use of passwords, logging-off, use of content, research skills, copyright
- 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

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Staff and Governors

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Governors are invited to online safety training events.

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
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements
- The Online Safety Coordinator will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy will be presented to and discussed by staff in staff meetings
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required

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 on-line 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:

- Letters, newsletters, website
- Displays in school / at parents' evenings
- Parent / carer online safety workshop
- High profile events and campaigns such as Safer Internet Day
- Reference to the relevant websites / publications for further support

Managing the Infrastructure, Equipment and Content

Access, Security and Filtering

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

- The school network has user-defined policies ensuring secure documents are only accessible by specific users
- The school has educational, filtered, secure broadband connectivity
- Internet access is filtered for all users to keep users safe, including from terrorist and extremist material. Illegal content is filtered by the broadband provider, and only nominated staff are able to make a change to the filtering system
- The school will ensure, to the best of their ability, that the filtering system prevents pupils using websites designed to bypass the filtering
- The school has a secure wireless network to ensure access is restricted to school devices

- If staff or pupils come across unsuitable on-line materials, the site is reported to the appropriate person(s) in line with school policy
- The school checks their virus protection is updating regularly and informs their IT Support Service provider of any issues
- Staff and pupils have access to the school network via a login suitable to their 'role'. Staff do not share their login details.
- Staff access to the management information system is controlled through a separate password for data security purposes. Staff only have access to the modules they require for their role, and passwords are not shared
- The school checks that their data is backed up
- The school 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
- Guest accounts are only used for a short period of time by temporary staff
- Guest access to wifi is only accessible with a guest password which is changed regularly
- The school requires all users to log off when they have finished working, and to log off (or lock if not a shared computer) when leaving the computer unattended
- The school ensures that all pupil level or personal data sent over the internet is encrypted or sent using an approved system, for example DfE S2S, Egress secure file / email
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
- Pupils use a child-friendly internet search engine

Password Policy

- The school makes it clear that staff and pupils must always keep their passwords private and not share them with others
- If a password is compromised the school should be notified immediately
- Staff are required to use strong passwords for network / email / MIS
- Staff are required to change their email / MIS passwords at least twice a year

Personal Devices

- Personal devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school
- Staff should not use their personal device when contacting pupils or parents; there should be access to a school phone
- The school does not allow pupils' mobile phones to be brought into school, with the exception of Year 6 to use on their journey to and from school.
- The recording, taking and sharing of images, video and audio on any personal device is strictly prohibited, except where it has been explicitly agreed otherwise by the headteacher
- The school reserves the right to search the content of any mobile or handheld device on school premises where there is a reasonable suspicion that it may contain undesirable material
- Personal devices will not be used during lessons unless as part of an approved and directed curriculum-based activity

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- The school 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 within unnecessary delay
- The Headteacher is the Senior Information Risk Officer
- Staff must ensure that at all times they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Staff must 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
- Staff must ensure they only transfer data using encryption and secure password protected devices

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 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
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Digital media should be used in accordance with the home school agreement
- The digital media release form should be reviewed annually
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- 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. 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. Personal equipment of staff should not be used for such purposes
- Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website will be selected carefully and will comply with good practice guidance on the use of such images

Email and Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Schools need to consider the benefit of using these technologies for education whilst reducing their risks.

- Staff should only use the school email service to communicate with others when in school, or on school systems. Users should be aware that email communications are monitored
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content, and must only take place on school approved systems. Personal email addresses or social media must not be used for these communications
- Users must immediately tell an appropriate member of staff if they receive any communication which is offensive, discriminatory, threatening or bullying in nature, and should not respond to any such communication
- Staff or pupil personal contact information should not be published. The contact details given online should be the school office
- Pupils should be taught about online safety issues such as the risks attached to the sharing or 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
- In all communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Pupils need to be educated in how to deal with incoming email and associated attachments
- The school should consider how e-mail from pupils to external bodies is presented and controlled

Social Media – Staff (Protecting Professional Identity)

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability 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 has clear reporting guidance, including responsibilities, procedures and sanctions
- All school staff sign the Acceptable Use Agreement indicating they understand and will follow the guidance contained
- School staff ensure they make no reference in social media to pupils, parents / carers or school staff
- School staff should not engage in online discussion on personal matters relating to members of the school community
- School staff should ensure that personal opinions are not attributed to the school or local authority
- School staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- As part of active social media engagement, it is considered good practice to proactively 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

Social Media – Pupils

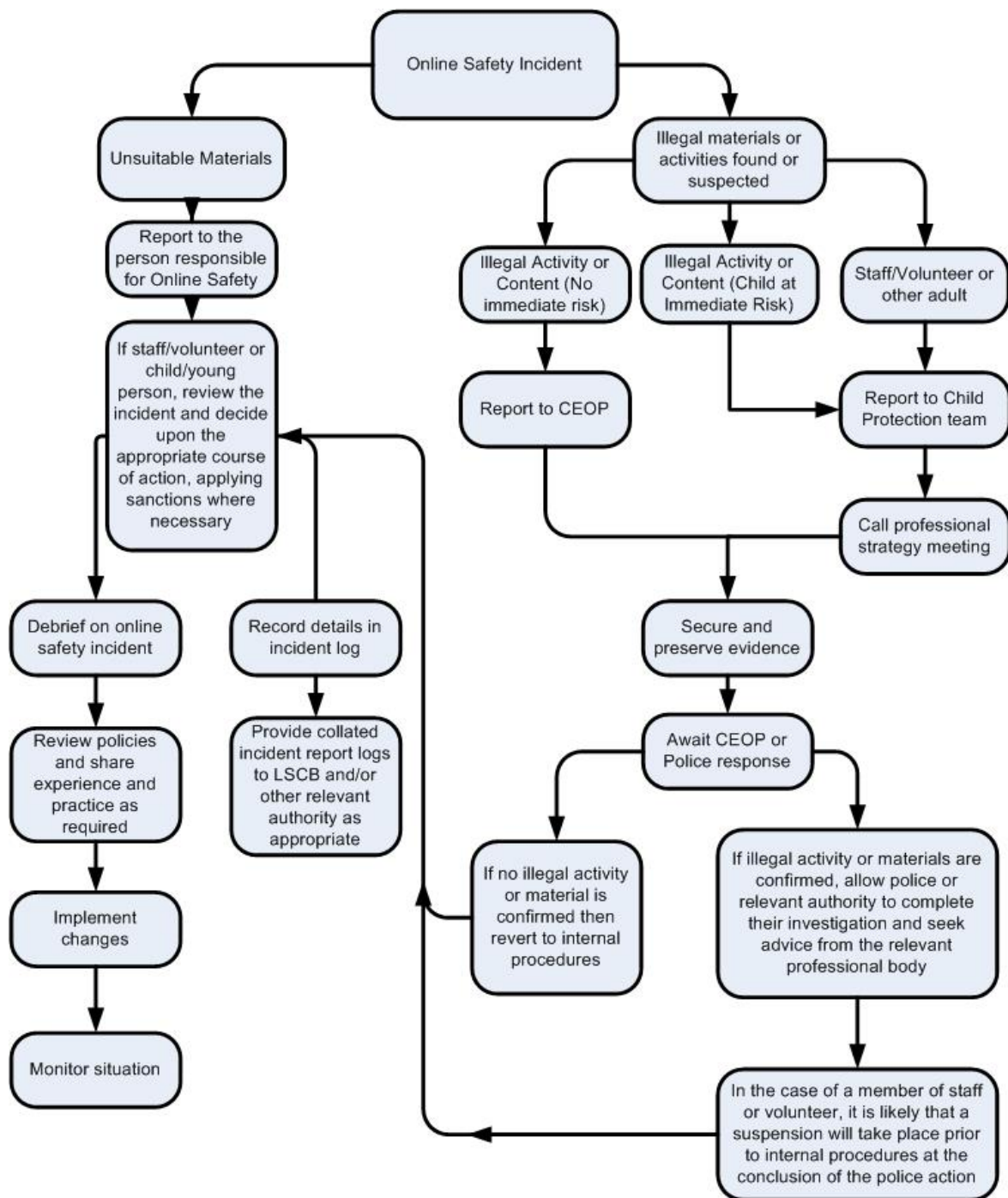
- The school will control access to social networking sites, and where relevant educate pupils in their safe use
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils
- Pupils will be advised to use nicknames and avatars when using social networking sites

Incident Management

Responding to Incidents

- The school will take all reasonable precautions to ensure online safety
- Complaints of internet misuse will be dealt with by a senior member of staff, with Online Safety Coordinator as first point of contact
- Any complaint about staff misuse must be referred to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the Local Authority's Designated Officer
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- If a member of staff or pupil receives online communication that is considered particularly disturbing or illegal, the Police will be contacted
- If an incident involving sexting comes to the attention of a member of staff, it must be reported to the Designated Safeguarding Lead immediately (see appendix 2 for further advice relating to sexting incidents)
- Complaints related to cyberbullying will be dealt with in accordance with school bullying procedures
- Monitoring of incidents takes place and contributes to developments in policy and practice in online safety within the school
- Parents / carers are informed of online safety incidents involving children and young people for whom they are responsible

Responding to Incidents – Flow Chart



Appendix 1

Online Safety in Computing Programme of Study

Key Stage 1

Pupils should be taught to:

- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2

Pupils should be taught to:

- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Use technology safely, respectfully and responsibly; recognise acceptable / unacceptable behaviour; identify a range of ways to report concerns about content or contact

Key Stage 3

Pupils should be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns

Key Stage 4

Pupils should be taught to:

- understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns.

Appendix 2

Handling a Sexting Incident

An overview for all teaching and non-teaching staff in schools and colleges

UK Council for Child Internet Safety (UKCCIS)

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as the **production and / or sharing of sexual photos and videos of and by young people who are under the age of 18**. It includes nude or nearly nude images and / or sexual acts. It is also referred to as 'youth produced sexual imagery'.

Sexting does not include the sharing of sexual photos and videos of under 18-year olds with or by adults. This is a form of child abuse and must be referred to the police.

What to do if an incident involving sexting comes to your attention:

- **Report it to your Designated Safeguarding Lead immediately**
- **Do not** view, download or share the imagery yourself, or ask a child to share or download
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL
- **Do not** delete the imagery or ask the young person to delete it
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- **Do not** share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers
- **Do not** say or do anything to blame or shame any young people involved
- **Do** explain to the child that you need to report it and reassure them that they will receive support and help from the DSL

For further information:

[Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People](#) (UKCCIS, 2016)