Victoria Primary School
Online Safeguarding Policy
Updated September 2018

Believing and achieving together

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Radicalisation and extremism
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- Child sexual exploitation
- Sexting
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying including prejudiced-based bullying, for example, peer on peer abuse, homophobic bullying, racist bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The Online Safeguarding Team

Jackie Renton – Deputy Head / Online Safeguarding Lead / ICT Leader / Designated Safeguarding Lead (DSL)

Jane Dark – Headteacher / Deputy Designated Safeguarding Lead (DDSL)

Wayne Smith – Assistant Head / Deputy Designated Safeguarding Lead (DDSL)

Sarah Scott – Assistant Head / Deputy Designated Safeguarding Lead (DDSL)

Kathryn Jones - Inclusion Lead (SEND) / Deputy Designated Safeguarding Lead (DDSL)

Members of the school's Junior Leadership Team Behaviour and Safety Committee

Our school technician is Mohammed Saleem. The team will consult him over technical issues related to safeguarding and security of data.

Development and Review of this policy.

This Online Safeguarding Policy was reviewed by the Governors' School Improvement Committee	26.11.18
The implementation of this Online Safeguarding Policy will be monitored by the:	Governors' School Improvement Committee
Monitoring will take place at regular intervals:	Annually
The Online Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	November 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Children's services 01274 437500 (or 01274 431010 out of hours team) Bradford Learning Network - 01274 434825 Police Javelin House Child Protection Unit 01274 376061

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported incidents in the e-safeguarding incident log kept in the Online Safeguarding Leader's office
- Internal monitoring data for network activity -Jackie Renton - ICT Leader / Deputy Head / DSL
  and Jane Dark – Headteacher / DDSL

- Smoothwall monitoring of network activity including forensic keystroke monitoring of all machines.

- Online safety meetings as part of Junior Leadership Team meetings

- A forensic monitoring service monitors the school network as part of the schools Bradford Learning Network (BLN) subscription. Jackie Renton receives emails weekly to report on any inappropriate activity, or not, on any computer in school. Any activity report is followed up immediately. Parents are contacted and informed of the incident and the child meets with the Headteacher and/or Deputy Headteacher to discuss the safety implications of their actions.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors School Improvement Committee receiving regular information about online safety incidents and monitoring reports. The Governor responsible for Child Protection and Safeguarding, including Online Safeguarding is Sandra Firm.

The role of this governor will include:

- regular meetings - which will include Safeguarding where online safety issues will be discussed
- regular monitoring of online safety incident logs - forensic science software logs
- reporting to relevant Governors through minutes of the School Improvement Committee

Headteacher and Senior Leaders:

- The Headteacher is responsible 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 Online Safeguarding Leader Jackie Renton.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safeguarding Leaders and other relevant staff receive suitable CPD to enable them to

carry out their online safeguarding roles and to train other colleagues, as relevant.

- The Headteacher and Online Safeguarding Leader are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. This is detailed in the Safeguarding Policy.

Online Safeguarding Leader:

- Takes day to day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the school online-safeguarding policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports to the Governors School Improvement Committee via the Headteacher.
- Trains staff on online safeguarding annually as part of child protection / safeguarding training.
- Organises online safety events for children.
- Keeps up to date with Local and National online safety issues and disseminates to staff, children and governors as appropriate and necessary.

Training Network Manager / Technical staff:

Mohammed Saleem the school technician ensures:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That he keeps up to date with online safety technical information and updates the Online Safeguarding Leader as appropriate.
- That monitoring software and anti-virus software is implemented and updated and supports with any safeguarding issues that may arise.
- Liaises with the Online Safeguarding Leader on a weekly basis.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safeguarding matters and of the current school Online Safeguarding Policy.
- They have an understanding of when to make referrals when there are issues concerning sexual exploitation, radicalisation and/or extremism.
- They understand the risks posed by those who use technology, including the internet, to bully, groom, radicalise or abuse children or learners.
- They know where to seek professional advice and support.
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Online Safeguarding Leader for

investigation.

- Digital communications with students / pupils (eg email) should be on a professional level and only carried out using official school systems as outlined in this policy.
- Online safeguarding issues are embedded in all aspects of the curriculum and other school activities.
- Online safeguarding lessons are taught across all year groups.
- Online safeguarding lessons are planned and taught every half term and that the lessons are age appropriate / reflect the needs of the age group and are an ongoing part of everyday online activities.
- Pupils understand and follow the school Online Safeguarding and Acceptable Use policies.
- They are aware of online safeguarding issues related to the use of mobile phones, cameras and hand held devices; they monitor their use and implement current school policies with regard to these devices.
- Any external confidential files are sent by an encrypted email system called Galaxkey.

Designated Safeguarding Lead

Jackie Renton (DHT) is the Designated Safeguarding Lead, Jane Dark (HT), Wayne Smith and Sarah Scott (AHTs) and Kathryn Jones are the Deputy Designated Safeguarding Leads. They are trained in online safeguarding issues and are aware of the potential for serious child protection issues to arise from:

- Radicalisation and extremism
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- Child sexual exploitation
- Sexting
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying including prejudiced-based bullying, for example, peer on peer abuse, homophobic
  bullying, racist bullying, sexual harassment
- Access to unsuitable video / internet games
- Illegal downloading of music or video files

Children

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to sign annually before being given access to school systems.

- Pupils are encouraged through online safeguarding/PSHE lessons to share any online safeguarding concerns with a trusted adult
- Are taught to understand, respond to and calculate risk effectively.

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to online safety. We will assist parents to understand key issues in the following ways:

- A parents' online safety presentation delivered by local community police on an annual basis.
- There will be an online safeguarding element to the parents' meetings which take place termly.
- Curriculum information sent to parents half termly also covers online safeguarding.
- Regular newsletters offer parents advice on the use of the internet and social media at home.
- Parents are asked to discuss the pupil acceptable use policy with their children and are expected to sign their child's diary to say they have done so.

Community Users

Community Users/ visitors and volunteers will inform the Deputy Head / Online Safeguarding Leader of any web sites they wish to access. No person can log on to the internet without a user account or the Internet password.

Education - Pupils

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

Online safeguarding education will be provided in the following ways:

- A planned online safety programme is delivered as part of PHSE.
- Staff highlight online safeguarding issues that arise in the context of ICT lessons and across the curriculum.
- Key online safety messages are reinforced as part of a planned programme of assemblies. They take place at least once a term.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Rules for the use of ICT systems will be posted in all rooms and displayed on log-on screens. Pupils will sign a copy of the Acceptable Use Policy on entry into school.
- For directed searches in school, staff direct children to a search engine or other appropriate search tools.
- In upper KS2 pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education - Staff Training

It is essential that all staff receive online safeguarding training and understand their

responsibilities, as outlined in this policy. Training will be offered as follows:
A staff meeting covering online safety will take place annually. This will be delivered by the Online Safeguarding Leader and/or other relevant person for example, the local PCSO.
Online safeguarding forms part of the annual safeguarding and child protection training received by all staff.
All new staff receive online safeguarding training as part of their induction programme, ensuring that they fully understand the school online safeguarding policy and Acceptable Use Policies.
The online safeguarding leader has been trained as a ThinkUKnow Trainer. They are qualified to deliver CEOP Think U Know sessions to children and receive regular updates on practice through the CEOP web site.

Education - Governor Training
Governors should take part in online safety training / awareness sessions. Governors are invited to child protection and radicalisation training to enable them to keep informed. This will be delivered by the online safeguarding leader.

Internet Provision
The school Internet is provided by the Bradford Learning Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity.

Use of digital and video images - Photographic, Video

- 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 online.
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Photographs of children published on the website must not contain full names.
- Pupils' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Personal Data Protection
Staff must ensure that they follow the school GDPR policy and procedure and:

- At all times 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 of data is only done using encryption and secure password protected devices

such as

memory sticks.

- Staff always lock computers when unattended.

Passwords

All users (adults and children) will have responsibility for the security of their username and password; must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Passwords for new users, and replacement passwords for existing users, can be allocated by Jackie Renton or Mohammed Saleem.

Members of staff will be made aware of the school's password expectations:

- at induction
- through the school's Online Safeguarding Policy
- through the Acceptable Use Agreement

Children will be made aware of the school's password expectations:

- in ICT and / or online safety lessons
- through the Acceptable Use Agreement

All users will be provided with a username and password by Jackie Renton or Mohammed Saleem who will keep an up to date record of users and their usernames.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Then staff should immediately follow the guidance highlighted in 'Actions upon discovering inappropriate or illegal material'. It is important that the device is not shut down as evidence could be erased but that the machine is locked down and any content made inaccessible to anyone other than the SLT or ICT technician. All matters should be reported immediately to the Head/Online Safeguarding Leader.

If misuse has taken place which is not illegal it is important that any incidents are dealt with 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.
Whilst it is impossible to record possible sanctions for every eventuality all breaches of the ICT policies in school will be dealt with as deemed appropriate and may result in disciplinary action being taken or referral to the Police or other appropriate authority.

Cyber bullying including prejudiced based bullying
Cyber bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.
Pupils are taught about cyber bullying through Online Safeguarding and PSHE lessons. Pupils are encouraged to share concerns of cyber bullying with a trusted adult. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy. The school may report serious cyber bullying incidents to the Police.

Social Media
Victoria Primary School uses social media in the following ways:

- A text to parents system is used as a reminder service for parents. Only the SLT, Business Manager, Administrator or other delegated staff have login details and are authorised to use this.
- This system also sends emails to parents to send out information, for example, newsletters.
- Victoria Primary School has a Twitter account which publicises information such as trips, events and news.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school.

Mobile devices
Staff
Staff must not use mobile phones in lessons. During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' or 'discreet' mode. Except in urgent or exceptional situations, mobile phone use is not permitted during teaching time, while on playground duty and during meetings. Mobile phones should be kept in lockers and

not carried around school, with the exception of the senior leadership team who are required to carry their phones for emergency purposes, and the caretaking staff who are in various places across the site during the school day and may need to communicate with the SLT. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only School cameras or devices are to be used.

Pupils

School does not allow children to bring mobile phones or electronic devices into school or on educational visits. As part of our curriculum, pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly someone can post content online before thinking about the consequences.

School mobile devices

The school has a variety of mobile devices including iPods, iPads, flip cams, Easyspeak microphones, recordable buttons, digital cameras and laptops. All of the statements included in the Acceptable Use Policy apply to these mobile devices. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

We have detailed Acceptable Use Policies for staff and pupils and a separate acceptable use of cameras and mobile phones policy. This is included in the appendix of this policy.

Development and Review of this policy

The implementation of this policy will be monitored by the Online Safeguarding Committee. Monitoring of the policy will take place annually, or more regularly in light of any significant new developments in the use of technologies, new threats to online safety from incidents that have taken place.

Should serious online safety incidents take place, the following external persons/agencies should be informed: initial contact point Children's Services - 01274 437500, Bradford Learning Network – 01274 434835, Police Child Protection Unit - 01274 376061, E-ICT who manager our admin network – 01274 439300.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. (Regulation of Investigatory Powers Act 2000).

General Data Protection Regulation
Victoria Primary School – Nurture Academies Trust - Acceptable Use Policy 2018 Adult

Introduction

Victoria Primary School commits to protecting the privacy and security of the personal information it holds for staff, governors and volunteers. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This agreement covers all digital and physical data systems, e.g. the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.
2. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.
3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.

4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate. I will not use personal equipment to access school data.

5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.

6. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School system to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on the School system with any other user. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from sight. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.

7. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

8. I will respect copyright and intellectual property rights.

9. I have read and understood the school's Data Security Policy and Online-Safety Policy which cover the security of data and safe and appropriate access to data.

10. I will report all incidents of concern regarding children's online safety to the Designated Child Safeguarding Lead (DSL) / Online-Safeguarding Lead Miss J Renton and/or the Deputy Designated Safeguarding Leads (DDSL) Jane Dark (HT), Wayne Smith (AHT), Sarah Scott (AHT), Kathryn Jones (SENDCo) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the Online-Safety Coordinator.

11. I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.

12. My communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will ensure that a BCC of any emails to parents/carers are sent admin@victoria.bradford.sch.uk. All written notes will be copied to Mrs G Hudson. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership Team.

13. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.

14. My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, write, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

16. I will promote Online-Safety (including privacy) with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create. Similarly, I will promote care for others in the pupils' writing and any other content that they create.

17. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

18. The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

19. I agree to follow the school acceptable use of cameras and mobile phones procedure.

I ________________________________ (please print name) acknowledge that I have received and read and understood a copy of the Victoria Primary School Acceptable Use Policy.

Signed ______________________________

Dated ______________________________

Pupil Acceptable Use Agreement

These rules will keep me safe, keep my information private, and help me to be fair to others.

- ✓ I will only use the school's computers for schoolwork and homework.
- ✓ I will not attempt to read any personal information on paper or in a computer file unless that information is meant for me.
- ✓ I will only edit or delete my own files and not look at, or change, other people's files without their permission
- ✓ I will keep my logins and passwords secret.
- ✓ I will not attempt to learn logins and passwords that belong to other people
- ✓ I will not bring files into school without permission or upload inappropriate material to my workspace.
- ✓ I am aware that some websites and social networks have age restrictions and I will respect this.
- ✓ I will not attempt to visit Internet sites that I know the school has banned.
- ✓ I will only e-mail the people I know, or those a responsible adult has approved.
- ✓ The messages I send, or information I upload, will always be polite and sensible.
- ✓ I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- ✓ I will maintain my data and personal security: I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will *never* arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- ✓ If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- ✓ I will not bring a mobile phone into school except in exceptional circumstances and when specifically allowed by the Head Teacher.

I have read and understand these rules and agree to them.

Signed: ………………………………………… *Date:* ………………………

Acceptable use of cameras and mobile phone procedure

Mobile Phones

Victoria Primary School allows staff to bring in personal mobile telephones and devices for their own use.

Under no circumstances does the school allow a member of staff to contact a current pupil or parent/carer using their personal device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Staff must ensure that their mobile telephones/devices are left inside their bag throughout contact time with children. Staff bags should be placed in a secure place within the classroom, staff room or locker.

The Senior Leadership team are required to carry their mobile phone with them in school in case of an emergency such as a fire or other serious incident that requires evacuation of the school site, (see Emergency Plan). The caretaking staff also carry mobile phones as they are around the whole school site during the day and may need to contact / be contacted by the SLT.

Mobile phone calls may only be taken at staff breaks or in staff members' own time.

If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the office or the staff room.

If any staff member has a family emergency or similar and required to keep their mobile phone to hand, prior permission must be sought from the Headteacher.

Staff (will need to) ensure that the Headteacher has up to date contact information and that staff make their families, children's schools etc. aware of emergency work telephone numbers. This is the responsibility of the individual staff member.

All parent helpers will be requested to place their bag containing their phone in a secure area such as their personal locker, or another appropriate location and asked to take or receive any calls in the staffroom or office.

During group outings nominated staff will have access to their mobile phone, which is to be used for communication with school as necessary or emergency purposes.

It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher. Concerns will be taken seriously, logged and investigated appropriately (see allegations against a member of staff policy).

Mobile phones must not be used to take photographs of children.

Mobile phones must not be used to take photographs of children by parents in school or on school visits.

Mobile phones must not be used by staff to take photographs of other school staff on site, or when on school events, such as staff meals.

Cameras

Only school cameras must be used. The memory card should then be removed and the content loaded onto a school computer not a personal computer. Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form or recording their progression, but will only be shared according to school policy and permissions given by parents.

All staff are responsible for the location of the cameras other school equipment and are responsible for ensuring they are stored securely.

Images taken and stored on the photographic devices must be downloaded as soon as possible on to a school computer. Images must not be downloaded onto personal devices.

Failure to adhere to the contents of this policy could lead to disciplinary action being taken.

Photographs at school performances are not allowed. Opportunities are given to parents to take photographs of their own child at the end of any school performances.

Dealing with Online Safety Incidents

Action you must take if you discover inappropriate (threatening or malicious) material online concerning yourself or your school:

All online safety incidents are recorded in the School Online Safety Log (located in the Online Safeguarding Leaders office, which is regularly reviewed.
Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the Online Safeguarding Leader - Jackie Renton, or the Headteacher who will then respond in the most appropriate manner, possibly taking the following steps:

- Secure and preserve any evidence. For example, note the web address (URL) or take a screen shot or copy and print the screen
- Inform the Designated Safeguarding Lead (DSL) or Deputy (DDSL) - Jackie Renton (DSL) Jane Dark (DDSL), Wayne Smith (DDSL), Sarah Scott (DDSL), Kathryn Jones (DDSL).
- If appropriate, inform the Police Child Protection Unit - Javelin House - 01274 376061
- If appropriate contact parents

Instances of online bullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.
Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safeguarding Leader, Jackie Renton, and Technician Mohammed Saleem, and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.
School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer this must be immediately referred to the Headteacher and Online Safeguarding Leader. It is a criminal act under Section 1 of the Protection of Children Act 1978 for any person to make and distribute indecent images of children. These are arrestable offences.

Upon the receipt of any information concerning a person who is suspected of accessing indecent images of children online, the Headteacher should notify the Police (Child and Public Protection Unit) immediately. The computer should be left and not used by anyone, allowing this to be seized as evidence for forensic examination by the Police. The details of all persons having access to the computer should be made available to allow a clear evidence trail to be established.

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims

- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing, downloading and disseminating any material deemed inappropriate, offensive, obscene, defamatory, racist, homophobic, violent, promoting radicalization and/or extremism
- continuing to send or post material regarded as harassment or of a bullying nature after being warned
- staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is illegal, offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 1998

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during school hours
- accessing non-educational websites (e.g. gaming or shopping websites)
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else