GOOSE GREEN PRIMARY SCHOOL

Life, Learning and Laughter

Online Safety and Information Security Policy

Date: Spring 2017

Review Date: Spring 2019

1. Introduction

This policy is designed to ensure that children, young people and staff are able to use the internet and related communications technologies appropriately and safely, and that the information that the School holds is managed securely in accordance with the Data Protection Act.

The School's arrangements for processing personal information, including where information might be shared with other organisations, are set out in the School's *Data Protection Policy*.

If you don't comply with this policy, you may be subject to disciplinary action under the School's Code of Conduct (refer to the School's Disciplinary procedure for details of this). Where pupils do not comply with this policy action may be taken under the School's Behaviour Policy or Anti-Bullying Policy if appropriate.

1.1. Online safety

The internet offers children a valuable learning resource and important opportunities to discover more about their world and engage with other people. It is, however, essential that children and young people learn to use the internet safely and are protected from potential harm, both within and outside of school.

1.2. Information security

The School is trusted with handling sensitive and personal information from parents, carers, children, staff, partners and suppliers. **We all** have a responsibility to keep this safe. If we don't, children and the School could be put at risk.

The School's ICT support service is responsible for the implementation, maintenance and management of technical security controls defined in separate ICT security policies and procedures.

However, most losses of sensitive information happen when people misplace documents or devices (eg laptops, papers etc), mistakenly share it with the wrong people (eg by email or fax), or don't dispose of it safely.

This means that **we all** have a vital role to play in keeping information safe.

2. Scope of the Policy

This policy applies to all members of the School community (including staff, pupils, volunteers, parents / carers and visitors / other users) who have access to the School's ICT systems and information held by the School (including where information is held in paper records). This policy applies both in and out of the school.

This policy reflects the School's responsibilities under the Data Protection Act (1998), Education and Inspections Act (2006) and Education Act (2011) and has links with the School's Child Protection Policy and Procedure, Behaviour Policy and Anti-Bullying Policy.

3. Roles, responsibilities and requirements for online safety and information security

This section outlines the online safety and information security roles and responsibilities of individuals and groups within the School:

3.1. Governors / Board of Directors:

Governors are responsible for the approval of the Online Safety and Information Security Policy.

A member of the Governing Body will be assigned the role of Online Safety Link Governor. The Online Safety Link Governor will attend bi-annual meetings with the PSHE Lead, ICT Coordinator and ICT service provider which will include:

- Review of online safety incident logs.
- Review of activity to ensure that the School's ICT arrangements are complying with the Online Safety and Information Security Policy.

Updates will be provided to the Governing Body through the Business Operations Committee.

3.2. Headteacher and Deputy Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The Deputy Headteacher supports the Headteacher in fulfilling this duty of care. The day to day responsibility for online safety will be delegated to the PSHE Lead, ICT Coordinator and ICT support provider.

- The Headteacher and their Deputy Headteacher will ensure that they are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher is responsible for ensuring that the PSHE lead, ICT Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as required.
- The Headteacher will ensure that there are systems in place for monitoring of online safety and information security and reporting of suspected incidents.

3.3. Senior Leadership Team and Phase Leaders

The Senior Leadership Team and Phase leaders will:

- Ensure that they have an up to date awareness of online safety matters and have read, understood and comply with the School's *Online Safety and Information Security Policy* and associated practices, and promote the importance of this to other teaching and support staff.
- Receive regular monitoring reports from the PSHE lead and ICT Coordinator to ensure that they are aware of online safety and information security developments and any suspected incidents which have been investigated (including action taken in response to incidents).

3.4. PHSE lead

- Is a member of the Senior Leadership Team and leads the online safety group.
- Takes day to day responsibility for online safety issues and has a leading role in developing and reviewing the School *Online Safety and Information Security Policy* and guidance documents which are developed to support staff in understanding and following the policy.
- Ensures that all staff are aware of the *Online Safety and Information Security Policy*, what is required of them to follow the policy and procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff, including through PDMS / INSET days and by ensuring that all new staff receive online safety training as part of their induction programme so that they fully understand the School *Online Safety and Information Security Policy*. (This takes place annually during Safeguarding training and when the Code of Conduct policy is shared.)
- Leads development of a planned online safety curriculum as part of Computing, PHSE, other lessons and school assemblies, which should be regularly reviewed as part of the School's curriculum development.
- Ensures that the School is providing ongoing support and guidance for parents and carers regarding online safety, as described in section 3.10 below.

- Provides advice, guidance and training to other individuals (eg volunteers) as required.
- Liaises with the Local Authority / relevant body on online safety and information security matters.
- Liaises with the School's ICT Coordinator and ICT support provider regarding online safety matters.
- Receives reports of online safety incidents and maintains a log of incidents to monitor corrective actions and inform future online safety developments.
- Meets with the Online Safety Link Governor to discuss current issues, review incident logs and filtering / change control logs.
- Provides updates on online safety and information security matters to Governors through the Business Operations Committee.

3.5. ICT Coordinator

- Is the person designated to be the School's lead for the ICT support contract.
- Will ensure that the ICT support provider are aware of and implement and follow appropriate procedures in order to comply with the *Online Safety and Information Security Policy* and *Data Protection Policy*.
- Attends relevant meetings of Governors as part of the regular review of online safety and information security matters.
- Will ensure that there is a reporting link on the school website to http://www.ceop.police.uk/safety-centre so that parents or staff can report suspected abuse, sexual offenders or grooming.

3.6. ICT support provider

The School's ICT support provider is responsible for ensuring that:

- The School's technical infrastructure is secure and appropriately protected from misuse or malicious attack.
- The School meets required online safety technical requirements and any Local Authority / other relevant body online safety policy / guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy.
- An appropriate internet filtering policy is applied and updated on a regular basis.
- They keep up to date with online safety developments so that they are able to effectively carry out their duties in compliance with this policy and to inform and update others as relevant.

- The use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored so that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction, in line with School policies.

3.7. Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and have read, understood and comply with the School's *Online Safety and Information Security Policy* and associated practices.
- They consistently act as good role models in their use of digital technologies, the internet and computing devices (including mobile devices such as smartphones).
- They report any suspected misuse or concern to the Headteacher.
- Online safety issues (including use of digital photos, videos and other images) are embedded in all aspects of the curriculum and other activities, and pupils are taught about online safety issues and encouraged to adopt safe and responsible use of the internet and computing devices both within and outside school (including consideration of the risks attached to the sharing of personal details, images etc) wherever there is an suitable opportunity (not just in ICT lessons).
- Pupils are taught in all lessons to be critically aware of the materials / content they access online and guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies. (This includes ensuring that pupils understand and follow the requirements of the School's *Online Safety and Information Security Policy*.)
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and be vigilant to ensure that use complies with this policy.
- In lessons where internet use is pre-planned pupils are guided to sites which have been checked as being suitable for their use and ensure that processes are in place for dealing with any unsuitable material that is found in internet searches.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a

situation, staff can request that the ICT support provider (or other designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.8. Designated Safeguarding Lead and Deputy Designated Safeguarding Leads

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

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate online contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

3.9. Students / pupils:

- Are responsible for using the school digital technology systems appropriately and following instructions from teaching staff.
- Must have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (particularly in upper KS2).
- Must 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 expected behaviour regarding the taking / use of images and cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies both in and out of school.
- Must not take, use, share, publish or distribute images of others without their permission.

3.10. Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and computing devices in an appropriate way. Many parents and carers may have only a limited understanding of online safety risks and issues, and 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 take every opportunity to help parents and carers understand these issues through Meet the Teacher evenings, updates in School newsletters, letters, the School website and information about national / local online safety campaigns / literature (eg promoting http://www.parentport.org.uk, www.saferinternet.org.uk and http://www.childnet.com/parents-and-carers).

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow the school's guidelines on the appropriate use of information and ICT. This includes:

- Digital and video images taken at school events.
- Their children's personal devices in the school.

4. Photography, video and images of children

Many school activities involve recording images as part of the curriculum, school activities, publicity or to celebrate an achievement. Photos of children taken for school purposes must be handled in accordance with The Data Protection Act 1998 (see guidance from the Information Commissioner's Office here: https://ico.org.uk/for-the-public/schools/photos/).

To comply with the Act it is essential that consent is obtained from the parent or carer of a pupil for any images to be taken or recorded (written permission from parents or carers will be obtained upon entering the school and therefore before any images / videos are taken or published on the school website or in other media). It is also important to take into account the wishes of the child, remembering that some children may not wish to have their photograph taken or be filmed.

In accordance with guidance from the Information Commissioner's Office, parents and carers 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). Parents and carers will be encouraged to show due consideration when using these (eg when deciding whether to post on social networking sites).

Using images for publicity purposes will require the age-appropriate consent of the individual concerned and their parent / carer. Images should not be displayed on websites, in publications or in a public place without their consent. Staff should also be clear about the purpose of the activity and what will happen to the photographs / images / video footage when the lesson or activity is concluded. Pupils' work can only be published with the permission of the pupil and parents or carers.

Students' / pupils' full names will not be used anywhere on a website, blog or other publication, particularly in association with photographs.

Photographs, video footage or other images of pupils should only be taken using school equipment for purposes authorised by the School and should be stored securely on School equipment.

Staff should ensure that a member of the Senior Leadership Team is aware of the proposed use of photographic/video equipment and that this is recorded in lesson plans. All photographs, video footage and other images should be available for scrutiny and staff must be able to justify the purpose for taking them.

Staff must remain aware of the potential for images of children to be misused to create indecent images of children and / or for grooming purposes. Therefore, careful consideration should be given to how activities which are being filmed or photographed are organised and undertaken. Particular care should be given when filming or photographing young or vulnerable pupils who may be unable to question how or why the activities are taking place. Staff must also be mindful that pupils who have been abused through the use of video or photography may feel threatened by its use in a teaching environment.

While digital imaging technologies have created significant benefits to learning, staff, parents / carers and pupils must remain aware of the risks associated with publishing digital images on the internet (including the risk of cyber-bullying and short or long term embarrassment. The School will inform and educate users about these risks to reduce the likelihood of the potential for harm.

5. Data and systems security: arrangements that the school will make

The School will take appropriate measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage of information that the School holds.

The school will:

- Comply with the requirements of the Data Protection Act and adopt a Data Protection Policy.
- Implement appropriate technical security measures to ensure that the School's systems are secure.
- Take steps to control physical security of information (eg keeping sensitive and personal information in records are all kept in a locked filing cabinet).
- Ensure that information is only used for the purpose(s) that it is provided (including where data is shared with the School by third parties).
- Establish a business continuity / disaster recovery plan to ensure that the School's information is protected against system failure.

- Train all staff on their responsibilities for data protection and information security (see section 5 below).
- Investigate any reported breaches of this policy should they occur.
- Report the details of any breaches and actions taken to the Governing body.

6. Data and systems security: requirements for staff

To keep the School's information secure when using its systems, information or data, **all staff must comply with the guidelines in this section**.

6.1. General requirements

You **must**:

- Make sure that you understand and comply with this policy and any other policies, guidelines or legislation specified within it when using the School's systems and data.
- Never attempt to circumvent the security arrangements that have been made to protect the School's information.
- Alert the Headteacher if you believe there has been a breach or potential breach of this policy.
- Take reasonable care to protect access to the School systems, information and data that you have access to, including ensuring that you:
  - never share your account password or access to your account with other people (including managers or other members of staff)
  - never use someone else's account to access the School's systems, information or data
- Be aware that the School will monitor the use of the communications tools and services that it provides to ensure compliance with this policy and other legal or regulatory requirements. This includes a record of the websites you visit (or attempt to visit) which can be reviewed if inappropriate use is suspected.
- Where there is a need to access information (eg emails or files) in another user's account or device, or to review monitoring information about use of the School's systems, a written request must be submitted to the ICT support provider, which must be approved by the Headteacher and Chair of Governors. The ICT provider will only process properly authorised requests and will keep a record of these.

6.2. Use of ICT equipment and devices

This section explains your responsibilities relating to any device that you use for your work (eg laptops, mobile phones, tablets, etc). This includes all devices you have been provided with by the School (work devices) and also any personal devices that you use for work purposes.

Why is this important?

The option to use a range of devices gives you greater flexibility wherever and whenever you need to do your work. However, you are responsible for making sure that any School related information which you access or store on any device you use is kept secure at all times.

Your responsibilities

General principles

For any device which you use to access or store the School's information (including phones, tablets and cameras), you **must**:

- Take reasonable precautions to protect it from unauthorised access, misuse, damage or theft.
- Make sure devices are locked and protected by a passcode or password when left unattended (if this function is available on the device).
- Notify the School office immediately if your device is lost or stolen so they can take appropriate steps to protect your account and any information stored on the device - you must not delay doing this as it could lead to sensitive information being lost.
- Report security concerns to the Headteacher if you believe that unauthorised people may have seen or accessed work-related information or data.
- Be aware of your environment and not access personal or sensitive information where it could be seen by unauthorised people (eg in a café or on public transport).
- Mobile phones and other devices are not permitted to be used in certain areas within the School site such as changing rooms and toilets.
- Use suitable security equipment (eg a 'Kensington Lock') or lockable storage to secure equipment in areas that are not protected by access controls (eg swipe access).
- Never use public printers or public cloud print services, as this could result in printouts of sensitive information being lost.

School devices

During work hours, the School expects you to use its resources to help you with your work. Reasonable personal use of School devices is permitted provided it complies with this policy, is not during teaching time and any associated policies and standards specified in it.

When using a School-issued device, you **must**:

- Sign out any shared devices (eg school cameras used for trips etc) and delete and data from the device (eg photos etc) once they have been saved for the intended use.
- Never allow other people, including family members, to use School equipment that has been issued to you.
- Never install software that is not from a trusted source, as this could introduce malware and information security risks to the device - if in doubt, you must contact the School office for advice.
- Be aware that the School is not responsible for, and does not support, any personal applications that you install on the device.
- Be aware that the School is not responsible for, and does not support, any personal data stored on the device.
- Be aware that the School may delete any personal data or applications that you have installed.
- Make sure you are using the latest operating system and security software - if you don't know how to download or install these, contact the School office.
- Return all School-issued ICT equipment to the School when you stop working for the School.

Personal devices

When using a personal device for work purposes, you **must**:

- Not use personal devices around children or parents.
- Not record images or video of children at any time on a personal devices.
- Be aware that the School is responsible for and remains the owner of its information, regardless of whether you store, process or transmit it on your personal device.
- Never download sensitive or personal information onto a personal device.
- Be aware that the School is not responsible for, and does not support, any personal devices.
- Be aware that if your device is lost or stolen, the School will take reasonable measures to protect any work-related information that may be stored on it.
- If necessary, this includes deleting ('wiping') all data on the device where this is enabled when you connect to the School's systems. The School does not accept any liability for any loss that you incur as a result (eg through loss of personal data on the device).
- Download available software updates promptly and use suitable anti-virus protection so your device and any information held on it is protected against viruses or other vulnerabilities.

- Never use non-standard versions of a device's operating system software (eg you must not 'jailbreak' or 'root' the device).
- Use an account that belongs to and is unique to you.
- Protect your device with a password that is at least:
    - eight characters long and contains numbers as well as letters (PCs and laptops)
    - six characters long (phones and tablets)
- Never use shared or public computers to access School information unless they are protected by an individual account that is used to access the computer, with a password that only you have access to.

The following additional requirements apply to the School's pupils:

- Pupils may bring mobile phones to school but must hand them in at the office for safekeeping.
- Pupils **must not** bring other devices such as tablets and games consoles into school.

USB removable media ('memory sticks')

When using USB removable media, you **must**:

- Only use encrypted USB media devices issued by the School.
- Do not use a USB device for general storage (they should only be used for a specific purpose and when there is no other alternative available).
- Delete your data from the USB device as soon as it is no longer needed.
- Never leave removable media unattended in an unsecure location.

6.3. Use of communications tools and services

This section explains your duties and obligations when using digital services, applications and extensions (eg Dropbox, webmail, Whatsapp etc).

<u>Why is this important?</u>

The School allows staff to use a range of communications tools and services to carry out their work, including online services provided by third parties. This means you can use such tools to plan, manage and deliver your work.

While this gives you the flexibility to use different services, you are responsible for making sure that any sensitive or personal information you use is kept secure at all times.

<u>Your responsibilities</u>

General principles

When using any communication tools, services, apps or extensions to access or store the School's information, you **must**:

- Be aware of, and comply with, any guidance provided for use of specific tools provided by the School (eg secure email services etc).
- Not use personal email addresses, text messaging or social media to communicate with children, parents or carers.
- Never attempt to access School systems or information for which you do not have authorised access, or which you ought not to have access to (eg if you discover you are able to access files that should not be available to you).
- Update any appropriate records so that there is a record of any points discussed / decisions made where required.
- Be aware that systems or online services that are not provided by the School might not be secure and might not protect the privacy of information - you MUST only use School-assured applications and services for sensitive and personal information.
- Be aware that agreements or contracts entered into electronically (eg by email) are as binding as written documents (it is your responsibility to ensure that the content of communications are correct).
- Take reasonable care to ensure that your communications are addressed / directed to the intended recipients (eg making sure that you use the correct email addresses).
- Take reasonable steps to make sure that the person you are communicating with is who they say they are and that they are authorised see any information you are sharing.
- Take reasonable care when communicating with untrusted and / or unknown contacts.
- Never click links to web addresses (URLs) or open attached documents received from untrusted or unknown sources or contacts.
- Never send sensitive or personal information to your personal email account, personal cloud storage service (eg Dropbox, Box.com, SugarSync etc), or other services or systems that are not provided by the School (eg Facebook, Whatsapp etc).

Instant messaging, SMS ('text' messages), video chat and telephone

When you use communications services (eg phone, Skype etc), you **must**:

- Make sure you can't be overheard if you are discussing information that is sensitive in any way (eg you must never discuss sensitive or personal information in a cafe or on public transport).

- Make sure your camera isn't positioned in such a way that it could accidentally film sensitive documents or computer screens on nearby desks.
- Make sure your microphone isn't positioned so it can pick up sensitive conversations taking place nearby.
- Check if the conversation is being recorded. If it is, you must treat the recording in the same way as written communication.

Online posting, including social media

When posting content online (eg comments, status updates, photos, links, videos etc), you **must**:

- Be aware that you are personally responsible for all content that you publish online.
- Never post sensitive or personal information which may put individuals or the School at risk, and not make references to pupils, parents / carers or school staff.
- Only use official email addresses / contact information when posting posting on behalf of the School.
- Never share sensitive or personal information on a public forum or other online service that has not been assured by the School as secure.
- Make sure you have permission to publish content that may be protected by copyright, fair use or financial disclosure laws.
- Behave appropriately and professionally, with the understanding that you are representing the School. This includes written content, videos or photographs and views expressed either directly or by 'liking' certain pages or posts or following certain individuals or groups. You must also exercise care when using dating websites where you could encounter past and present students.
- Not make contact with pupils or their family members (including not accepting or initiating friend requests nor follow pupil's or their family members' accounts) on any social media platform. The only acceptable method of contact is via the use of school email accounts, school telephone equipment or other communications services that the school provides.
- Goose Green Primary and Nursery School acknowledges that staff who are also parents may wish to make contact with other parents, who are friends, over social media. In these circumstances staff must exercise caution and professional judgement and should not have any contact with pupils' family members via social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- Alert the Headteacher immediately if the press or media contact you about anything you have posted online.

6.4. Use of the internet

This section explains your duties and obligations when using internet services provided by the School or accessing the internet through School-issued devices.

<u>Why is this important?</u>

Access to the internet is provided to assist you with your work and you have a duty to protect any sensitive or personal information that you access while using the internet.

If you don't take steps to keep the School's systems, information and data safe by using the internet responsibly and following this policy, it could put children and the School at risk.

<u>Your responsibilities</u>

During work hours, the School expects you to use its resources to help you with your work. Reasonable personal use of the internet is permitted provided it complies with this policy, is not during teaching time and any associated policies and standards specified in this policy.

When using internet services provided by the School, or accessing the internet through School-issued devices, you **must**:

- Be aware that the School uses filtering software to automatically block access to some websites which it considers inappropriate or a potential security risk.
- Never download or stream video, music files, games, software files or other computer programs that do not relate to your work - these types of files consume large quantities of internet bandwidth, storage space and may violate copyright laws.
- Never deliberately view, copy or circulate any material that:
    - is sexually explicit or obscene
    - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
    - contains images, cartoons or jokes that may cause offence
    - contains material the possession of which would constitute a criminal offence
    - promotes any form of criminal activity
- Contact the School office immediately if you accidentally visit a site which contains material that might be deemed illegal, obscene or offensive (see list above) so that it can be added to our list of blocked sites.

- Be aware that if you use the School's internet services for personal use (eg for online shopping), the School will not accept liability for default of payment, failure to provide services, or for the security of any personal information you provide online.

6.5. Documents and paperwork

This section explains your duties and obligations for keeping documents and paperwork secure.

Why is this important?

The security of documents and paperwork is just as important as electronic information. It is essential that this information is managed securely as otherwise children and the School could be put at risk.

Your responsibilities

When working with documents or other papers containing sensitive or personal information, you **must**:

- Never leave papers unattended, especially in areas where they could be seen by unauthorised people.
- Keep papers in locked storage (eg a locker or cabinet) when not in use.
- Take reasonable measures to keep papers secure if you take them away from the School's premises.
- Dispose of papers containing sensitive or personal information securely by using a secure waste bin or shredder.
- Return to the School any information held on paper or non-School services / systems when you leave.
- Never write down or print off any passwords or codes that allow access to systems or services that use or store work-related information (if you need to keep a record of your passwords, you must use a password-protected document or an approved password storage application).
- Report security concerns to the Headteacher if you believe that unauthorised people may have seen or accessed School information or data.

7. Managing incidents and suspected breaches of this policy

When an incident or suspected breach of this policy occurs then it is essential that this is investigated promptly and thoroughly, with appropriate steps taken to ensure the safeguarding the welfare of any children and any other people involved.

7.1. All incidents and suspected breaches

Where an incident or suspected breach of this policy occurs it must be reported to the PHSE lead. They will ensure that the incident / suspected breach is investigated, including:

- Gathering and preserving any evidence so that it is available for any further investigation.
- Ensuring that appropriate action is taken to mitigate the impact of the incident / potential breach as quickly as possible (including liaising with the ICT Coordinator and ICT support provider so that any required technical measures are taken to protect the School's system and information).
- Maintaining a record of the investigation and action taken for reporting and review purposes.
- Referring the incident / suspected breach to the Headteacher / Designated Safeguarding Lead (or Deputy) where it is identified that action might be required under the School's Code of Conduct / Disciplinary process or *Child Protection Policy* and *Child Protection Procedures*.
- Supporting the Headteacher / Designated Safeguarding Lead (or Deputy) where any further investigation is required.

7.2. Incidents and suspected breaches involving illegal content or presenting potential safeguarding concerns

Where an incident or suspected breach of this policy involves content that might be illegal or which might present safeguarding concerns then the incident must be managed in accordance with the School's *Child Protection Policy* and *Child Protection Procedures*.

The incident must be reported immediately to the School's Designated Safeguarding Lead (or Deputy) who will be responsible for the subsequent investigation and taking any action required.

ADOPTED AND SIGNED ON BEHALF OF THE SCHOOL GOVERNING BODY:	Ruth Kettell
SIGNATURE OF GOVERNING BODY REPRESENTATIVE:	
NAME OF HEADTEACHER:	Annabelle Birleanu
SIGNATURE OF HEADTEACHER:	
DATE:	Spring 2017
REVISION DATE:	Spring 2019