West Norfolk Academies Trust

Online Safety Policy

Incorporating Mobile & Smart Technology

Approved By:	Governing Body
Approval Date:	April 2024
Review Date:	April 2026

Contents

1. Purpose and Aims

1.1 Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

2.1 This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

2.2 It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

The Local Governing Body

3.1 The local governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

3.2 The local governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.3 The local governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

3.4 All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that all staff undergo safeguarding training to include online safety and that this includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Do all that they reasonably can to limit children's exposure potentially harmful and inappropriate online material on the school's IT system.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

3.5 The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

3.6 Details of the school's DSL and deputies are set out in our safeguarding policy, as well as relevant job descriptions.

3.7 The DSL takes lead responsibility for online safety and understanding the filtering and monitoring systems and procedures in place in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Trust IT staff and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety ensuring that relevant staff have an awareness and understanding of the provisions in place in regards to filtering and monitoring and that they manage them effectively to know when to escalate concerns identified.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- To be responsible for ensuring the standards in the DFE Filtering and Monitoring documentation are met.

West Norfolk Academies Trust (WNAT) IT Team

3.8 The WNAT IT team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Helping to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Helping to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All Staff and Volunteers

3.9 All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Having an understanding of the expectations, applicable role and responsibilities in relation to filtering and monitoring.

3.10 Parents/Carers are Expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use
- of the school's ICT systems and internet.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Use school systems, such as Google classroom, and other network resources, safely and appropriately.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.

Visitors and Members of the Community

3.11 Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read, agree to it and follow it.

4. Educating Pupils About Online Safety

4.1 It is essential that children are safeguarded from potentially harmful and inappropriate online material. We have an effective whole school approach to online safety that empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

4.2 At our school we ensure online safety is a running and interrelated theme. Pupils will be taught about online safety as part of a broad and balanced curriculum:

We recognise the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (eg consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

In **Key Stage 1**, pupils will 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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.*
- *How information and data is shared and used online.*
- *What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.*

In **Key Stage 3**, pupils will 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

Pupils in **Key Stage 4** will be taught:

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

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

The school will also use assemblies and other national days to raise awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating Parents/Carers About Online Safety

5.1 The school will raise parents/carers' awareness of internet safety through electronic communication and, when necessary, information evenings. This policy will also be shared with parents/carers via the website.

5.2 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

5.3 Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Procedures for Responding to Specific Online Incidents or Concerns

6.1 Cyber-bullying Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and Addressing Cyber-bullying

6.2.1 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.2.2 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

6.2.3 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes computing lessons and personal, social, health and economic (PSHE) education, along with other subjects where appropriate.

6.2.4 All staff, receive training on cyber- bullying, its impact and ways to support pupils, as part of safeguarding training

6.2.5 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

6.2.6 The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Consensual and Non-consensual Sharing of Nude and Semi-nude Images and/or Videos

6.3.1 The school recognises consensual and non-consensual sharing of nudes and semi-nudes and/or videos (also known previously as youth produced sexual imagery or "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

6.3.2 The school will ensure that all members of the community are made aware of the potential consequences of consensual and non-consensual sharing of nudes and semi-nudes and/or videos by implementing preventative approaches, via a range of age and ability appropriate educational methods.

6.3.3 The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

6.3.4 If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will act in accordance with our Child Protection and Safeguarding policies and Behaviour Policies

6.3.5 In line with DFE guidance: Sharing nudes and semi nudes: advice for education settings working with children and young people, if a member of staff is alerted to an incident they know, or suspect, is a nude or semi-nude picture they must never view, copy, print, share, store or save the imagery themselves, or ask a child to share or download – this is illegal.

6.3.6 The DSL will make a referral to children's social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process.

6.4 Online Child Sexual Abuse and Exploitation

6.4.1 The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

6.4.2 The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

6.4.3 The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.

6.4.4 The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

6.4.5 The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community through the school's website

6.5 Dealing with Online Child Sexual Abuse and Exploitation

6.5.1 If the school are made aware of an incident involving online sexual abuse of a child, the school will act in accordance with the school's Child Protection and Safeguarding Policies. It will:

- Immediately notify the Designated Safeguarding Lead;
- Store any devices involved securely;
- Immediately inform police via 101 (or 999 if a child is at immediate risk);
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies);
- Inform parents/carers about the incident and how it is being managed;
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support;
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

6.5.2 The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.

6.5.3 Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via CEOP.

6.5.4 If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the CADS and Norfolk Safeguarding Children Partnership.

6.5.5 If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the CADS by the Designated Safeguarding Lead.

6.5.6 If pupils at other schools are believed to have been targeted, the school will seek support from Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

6.6 Examining Electronic Devices

(This should be read in conjunction with the Trust Staff Code of Conduct: Section 18. Unacceptable Use of ICT Facilities and Monitoring)

6.6.1 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

6.6.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

6.6.3 Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

6.6.4 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable Use of the Internet in School

7.1 All pupils, parents/carers, staff, volunteers and governors who access the school system are agreeing to understanding and following the West Norfolk Academies Trust acceptable use of ICT policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

7.2 Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. In our schools we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered and monitoring standards.

7.3 E-mail

7.3.1 We provide staff with an email account for their professional use and make it clear that personal email should be through a separate account

7.3.2 We use anonymous e-mail addresses, for example head@, office@

7.3.3 Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

7.3.4 Will ensure that email accounts are maintained and up to date

7.4 Pupils Email:

7.4.1 We use school provisioned pupil email accounts that can be audited and which do not identify the child in the email address itself.

7.4.2 Pupils are taught about the online safety and 'etiquette' of using e-mail both in school and at home.

7.4.3 Pupils will sign an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.5 **Staff Email:**

7.5.1 Staff will use Trust or school provisioned e-mail systems for professional purposes

7.5.2 Access in school to external personal e-mail accounts may be blocked

7.5.3 Staff will not use email to transfer staff or pupil personal data unless it is protected with secure encryption. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

7.6 **School Websites**

7.6.1 The school’s website complies with statutory DfE requirements.

7.6.2 Most material is the schools’ own work; where others’ work is published or linked to, we credit the sources used and state clearly the author's identity or status;

7.6.3 Photographs of pupils published on the web do not have full names attached. We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website;

7.6.4 The school will post information about safeguarding, including online safety, on the website

7.6.5 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. (See Staff Code of Conduct Section 17)

7.7 **Management Information System Access and Data Transfer**

7.6.1 Teachers and office staff have access to the MIS.

7.6.2 Data on this system must not be copied or shared with any other person and kept confidential.

7.6.3 Staff must log out of the MIS or ‘lock’ the machine when they are not near the computer.

7.8 **Social Networking - Staff, Volunteers and Contractors**

7.7.1 The use of any school approved social networking (e.g School X Account or School Facebook account) will adhere to ICT Acceptable Use Agreement

7.7.2 Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Executive Headteacher.

7.7.3 All members of staff are advised not to communicate with or add as ‘friends’ any current or past pupils or current or past pupils’ family members via any personal social media sites, applications or profiles.

7.7.4 Any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Safeguarding Lead and/or the Headteacher.

7.7.5 If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.

7.8 Digital Images and Video

7.8.1 We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school

7.8.2 We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs

7.8.3 Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of personal mobile phones/personal equipment

Pupils:

Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work. Students are required to agree to and follow our pupil Acceptable Use Policy

Parents/Carers:

Parents/carers are reminded about social networking risks and protocols through our Acceptable Use Policy and additional communications materials when required.

Communicating with Pupils, Parents and Carers:

School will communicate with parents via approved official channels e.g. school website, email, school X account etc. All communication will comply with the Trust Data Protection Policy and Privacy Notices.

8. Artificial Intelligence (AI or Generative AI)

Generative AI refers to technology that can be used to create new content based on large volumes of data that AI models have been trained on from a variety of information from multiple sources.

Tools such as ChatGPT and Google Bard can:

- answer questions.
- complete written tasks.
- respond to prompts in a human-like way.
- Create images

However, the content produced by generative AI could be:

- inaccurate.
- inappropriate.
- biased.
- taken out of context and without permission.
- out of date or unreliable.

8.1 Caution should always be taken when installing applications on personal devices. Always make sure the app is from a reputable developer and fully understand the implications of any elevated access that the app is asking permission for.

8.2 Avoid sharing sensitive personal information through AI applications as this information could become part of the AI's information database and shared with others.

8.3 Report any suspicious or inappropriate use of AI technologies to school staff.

9. The Use of Personal Mobile Devices in School

9.1 Pupils using mobile devices in school (including smart devices)

9.2 The School understands that most students regularly use mobile phones, and will often need to use these on the way to and from school.

9.3 If a KS3 or KS4 pupil brings a mobile device into school it must be switched off upon arrival and before entering the school and not switched on again until they have left at the end of the school day. Mobile devices should be placed in school bags / lockers and not accessed in school at any time.

9.4 Mobile devices should not be used by pupils for any purpose within school unless express permission is granted by school staff (for example to monitor blood-sugar levels or to support their school work under the supervision of staff).

9.5 It is unacceptable to take a picture/video of a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images and will receive a behaviour sanction.

9.6 Mobile devices are banned from all examinations. Pupils must not bring mobile devices to any examination or controlled assessment. Pupils who arrive to examinations with a mobile device must hand it to the invigilator before entering the exam hall. The mobile device will be returned to the pupil after the examination. Any pupil found to be in possession of a mobile during an examination will be reported to JCQ (Joint Council for Qualifications) and risks being disqualified for that or all examinations.

9.7 The responsibility of looking after a mobile device (including a smart device) rests with the individual. If a pupil, parent or carer wishes for the school to look after the mobile device during the school day then this should be handed in following school procedures at the start of the day where it will be securely kept until the end of the day, and then returned to the student.

9.8 The school accepts no responsibility for replacing lost, stolen or damaged mobile devices or accessories.

9.9 Any unacceptable use of personal mobile devices in school will be addressed using the school’s behaviour policy.

10. The Use of Personal Mobile Devices and / or Online Software Outside School

Unacceptable use of mobile devices and/or online software outside of school will be addressed using the school’s behaviour policy.

11. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- If staff have any concerns over the security of their device, they must seek advice from the Trust ICT technician
- Keeping operating systems up to date by always installing the latest updates

- Staff members must not use the device in any way that would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.

12. How the School will Respond to Issues of Misuse

12.1 Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and Acceptable use of ICT policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

12.2 The DSL acts as the first point of contact for any safeguarding incident whether involving technologies or not.

12.3 Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with by the Headteacher, in accordance with the Staff Disciplinary Procedures and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

12.4 The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12.5 In our schools:

- there is strict monitoring and application of the Online Safety Policy, including the ICT Acceptable Use Policy and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within our schools
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the Trust
- for any breach of the acceptable use policy, the school will follow the agreed sanctions described in appendix 5 of this policy
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

13.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

13.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e- bulletins and staff meetings).

13.3 The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

13.4 Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

13.5 Volunteers will receive appropriate training and updates, if applicable.

13.6 More information about safeguarding training is set out in our safeguarding policy.

14. Monitoring Arrangements

14.1 The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

14.2 This policy will be reviewed annually. At every review, the policy will be shared with the governing board.

15. Links with Other Policies

This online safety policy is linked to our:

- Safeguarding Policy
- Behaviour policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT Acceptable Use Policy
- Examinations Policy

Appendix 1 – Recommended Organisations and Website

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites, for example

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- https://www.thinkuknow.co.uk/parents/
- https://www.saferinternet.org.uk/advice-centre/parents-and-carers
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childnet.com
- https://www.internetmatters.org