BOUGHTON PRIMARY SCHOOL: AN ACADEMY

An Academy

An Academy

Online Safety Policy and Procedures 2022-23

PERSON RESPONSIBLE FOR POLICY:	***MRS MARY JAMES***
APPROVED:	***APPROVED AT FGB MTG 22ND JUNE 2022***
BY:	***FULL GOVERNING BODY***
TO BE REVIEWED:	***ANNUALLY – JUNE 2023***

At *Boughton Primary* the named personnel with responsibility for Online Safety are:

Designated Safeguarding Lead	Deputy Designated Safeguarding Leads	Safeguarding Governor	Computing Lead	IT Technician
Mary James	*Jodie Hartwell* *Jenny Malcolm*	*Karen Wilson*	*Charlotte Page*	*ARK ICT*

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of Online Safety;
- work to empower the school community to use the internet as an essential tool for life-long learning.

This policy forms part of our Safeguarding Suite of policies and links closely with our Child Protection and Safeguarding Policy.

It is reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place, alongside any updates to legislation or guidance for schools.

Any breach of our agreed AUP for staff or pupils will be considered on an individual basis, according to age/stage for pupils and seniority of staff.

Although most possible breaches are covered by this document, anything considered to be inappropriate behaviour by pupils or staff will be dealt with accordingly.

Contents

Scope of policy	3
Schedule for Development, Monitoring and Review	3
Roles and Responsibilities	3-4
Curriculum	6
Education of wider school community	6
Training	6
Online Bullying	7
Sexting	7
Prevent	7
Technical Infrastructure	8
Data Protection	9
Use of digital and video images	9
Communication (including social media and use of own devices)	9-11
Reporting and Response to incidents	12
Sanctions and Disciplinary proceedings	13
Sanctions: Pupils	14
Sanctions: Staff	15
Useful Websites	16

Legislation and Guidance

This policy is based on the Department for Education'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

It also refers to the DfE's guidance on protecting children from radicalisation.

Our policy reflects existing guidance, including but not limited to the Education Act 1996, 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 cyber-bullying by, if necessary, searching for and deleting images or files on pupils' electronic devices where they believe there is "good reason" to do so.

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but linked to membership of the school. In addition, Keeping Children Safe in Education 2021 states very clearly that:

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face-to-face. In many cases, abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Keeping Children Safe In Education September 2021

This policy takes into account the National Curriculum computing programmes of study, and complies with our Memorandum and Articles of Association.

The Four 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, anti-Semitism, aggressive/violent/hateful content, radicalisation and extremism;
- ⇒ Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising, 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 scam.

Scope of policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, governors, visitors and community users.
The school will manage Online Safety as described within this policy alongside associated behaviour and anti-bullying policies and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

Purpose of policy

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children is paramount when any of our stakeholders are using the internet, on any device
- provide all members of our school community with overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our core values and within the law.

Schedule for Development, Monitoring and Review

The implementation of the Online Safety policy will be monitored by the governor with responsibility for safeguarding, who will discuss any concerns with the Head Teacher as part of the termly safeguarding checklist and report to the board at each full governors' meeting.

Roles and responsibilities

The **governing body** has overall responsibility for approving and monitoring this policy, and for holding the Head Teacher to account for its implementation.

The **Audit and Risk Committee,** and **Resources Committee** ensure that there is sufficient resource to maintain systems, which identify children accessing or trying to access harmful or inappropriate content online.

The **Learning and Outcomes Committee** monitor the curriculum, including the use of technology, and ensure that an appropriate online safety curriculum is taught.

The **Technical Support Provider** ensures that the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack. They ensure users may only access the school network through an enforced password protection policy. They maintain and inform the Head Teacher and School Business Manager of issues relating to filtering.
The Technical Support Provider is required to keep up to date with Online Safety technical information and update others as relevant; to ensure use of the network is regularly monitored in order that any misuse can be reported to the DSL for investigation; ensuring monitoring systems are implemented and updated. They ensure all security updates are applied (including anti-virus and Windows).

The **Head Teacher, senior leaders and all staff** oversee the safe use of technology when learners are in their care and take action immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The Head Teacher is the **Designated Safeguarding Lead** (DSL), supported by two **Deputy DSLs**. They have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying). They follow the correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil, in line with our Child Protection and Safeguarding Policy. They are responsible for informing MASH, the LADO and/or the police in the event of an allegation or serious issue.

The **Head Teacher** meets with the **Safeguarding Governor** in order to monitor the application of this policy, as part of the termly safeguarding checklist.

The **Head Teacher, senior leaders and the computing lead** ensure that all staff receive suitable CPD to carry out their online safety roles. This forms part of the annual safeguarding update, and is included where appropriate within the safeguarding element of the weekly staff meetings. They create a culture where staff, learners and parents feel able to report incidents.

With the support of the Head Teacher, the **Computing subject lead** ensures that there is a progressive online safety curriculum in place. They remain conversant with all aspects of online safety through reading, research and attending relevant meetings or training. They are responsible for cascading information about online safety to the staff team, parents and pupils in a timely way.

The **Computing subject lead** works with the **Senior Leadership Team** and the school's **technical support** to carry out an annual audit in order to review online safety. They ensure the implementation of this policy and related AUPs (Acceptable Use Policies), and agree an action plan to address issues arising.

Teaching and support staff are responsible for attending training or awareness raising sessions. They need to read, understand and sign the staff AUP, act in accordance with this and related policies. All staff are asked to be vigilant and to report any suspected misuse or concerns to the DSL, and to record these on My Concern.

Teaching staff need to provide appropriate online safety learning opportunities as part of a progressive online safety curriculum; they should model the safe and effective use of technology, and monitor ICT activities in lessons, extra-curricular and extended school activities.

All staff must demonstrate consistently high standards of personal and professional conduct, especially in relation to the use of social networks, making sure these are in line with the school ethos and policies, and with concern for the online reputation of the school.

Pupils are expected, as appropriate to their age/stage, to read, understand and sign the pupil AUP and agreed class rules. They need to participate in online safety activities, follow the AUP and report any concerns for self or others, including actions out of school that are related to their membership of the school (e.g. online conversations with children from school).

Parents and carers are asked to endorse, by signature, the pupil AUP; to discuss online safety issues with their child/ren, and to monitor their children's use of technology/the internet at home. They are asked to keep up to date with issues and information via the school's newsletters, website and any opportunities provided (e.g. meetings). Parents and carers are encouraged to inform the Head Teacher of any online safety issues that relate to the school. They are asked to maintain responsible standards if using social media to discuss school issues.

Visitors, volunteers and the wider community are asked to follow our guest AUP if accessing the school's internet, and to report any concerns to the Head Teacher.

Online Safety Curriculum

Our Computing Curriculum is aligned to the statutory requirements of the National Curriculum (2014), which states that pupils should be taught to:

KS1

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

KS2

use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

A progressive planned Online Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Breadth and progression is ensured through implementation of the 2014 curriculum update and Online Safety progression in line with national and local computing guides.
Within this:

- Key Online Safety messages are reinforced through assemblies, Safer Internet Week, Anti-Bullying week and throughout lessons, whenever opportunities arise

- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.

- Pupils are guided to use age-appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material

- In lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches

- Pupils are taught, through the e-safety curriculum and within their computing lessons, to be critically aware of the content they access online, including recognition of extreme and commercial content. They are guided to validate the accuracy and reliability 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 about current issues such as online gaming, extremism, vlogging and obsessive use of technology

- Pupils will write and sign an AUP for their class at the beginning of each school year, which will be shared with parents and carers

- Pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'.

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children and regular newsletter and website updates;

- raising awareness through activities planned by pupils;

- inviting parents to attend activities or other meetings as appropriate;

- providing and maintaining links to up to date information on the school website, on the Safeguarding and Wellbeing page.

Parents and carers are encouraged to contact the school if they have any queries or concerns in relation to online safety. The first port of call is their child's class teacher, who will refer on to the Designated Safeguarding Lead or Deputies if/when needed.

Visitors, volunteers and the wider community

Visitors, volunteers and members of the wider community are given a safeguarding leaflet on their first visit to the school, or on subsequent visits if it has been updated. They are expected to adhere

to our policies in terms of mobile phone use and are asked to report any concerns to the Head Teacher.

Training of Staff and Governors

Online safety forms part of our annual safeguarding/child protection briefing, and our bi-annual whole school training.

The Online Safety Leader (DSL) receives regular updates via online safety newsletters and related websites (e.g. NSPCC), which are shared and discussed as part of the safeguarding standing item in weekly staff meetings and termly governors' meetings.

The Online Safety Leader, in conjunction with the computing lead, provides guidance and training to staff as needed, and seeks support/advice from CEOP, the NSPCC and NSCP when required.

The telephone number for the UK Safer Internet Centre helpline is:
0344 381 4772

Online 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 one person or group by another person or group, where the relationship involves an imbalance of power.

Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. ***This includes incidents occurring either within or out of school.***

The school will follow procedures in place to support anyone in the school community affected by online bullying. Pupils, staff and parents are asked to report any concerns or issues to a trusted adult in school.

Pupils, staff and parents/carers will be encouraged to report any incidents of online bullying and advised to keep electronic evidence.

All incidents of online bullying reported to the school will be recorded by the school, using My Concern, and followed up by the DSL or Deputies accordingly.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's Online Safety ethos.

Sanctions and consequences for those involved in online bullying will follow those for other bullying incidents and may include:

- the perpetrator being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content in the event of refusal or difficulties removing content
- internet access being suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

Sexting

The school will provide appropriate support for sexting incidents, which take place in and out of school. Within school, any device that has an intimate sexting image or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead. An individual member of staff will not investigate, delete or pass on the image. The DSL will record any incident of sexting and the actions taken in line with advice from Northamptonshire Safeguarding Children Partnership.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking can be put into place.

Technical Infrastructure

The school ensures, when working with our technical support provider,that the following guidelines are adhered to:

- the School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements
- there are regular reviews and audits of the safety and security of school ICT systems.

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
  - the downloading of executable files by users
  - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school (see AUP)
  - the installing of programs on school devices
  - the use of removable media (e.g. memory sticks) by users on school devices.
  - the installation of up to date anti-virus software

- access to the school network and internet will be controlled by ensuring:
  - users have clearly defined access rights to school ICT systems through group policies
  - users, as appropriate to age, stage and role, are provided with a username and password
  - staff users are made aware that they are responsible for the security of their username and password, ***which they are required to change regularly***; they must not allow other users to access the systems using their log on details
  - the 'master/administrator' passwords are available to the Head Teacher
  - users immediately report any suspicion or evidence that there has been a breach of security
  - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this Online Safety policy
  - Key Stage 1 pupils' access is supervised with access to specific and approved online materials
  - Key Stage 2 pupils' access is supervised carefully. Pupils will use age-appropriate search engines and online tools and activities

- the internet feed will be controlled by ensuring:
  - the school maintains a managed filtering service provided by an educational provider that includes filtering of terms related to terrorism
  - the school monitors internet use, being aware of the websites that are used and attempts to access inappropriate or illegal sites

- requests from staff for sites to be removed from the filtered list are approved by the Technical Support and logged in writing
- requests for the allocation of extra rights to users to by-pass the school's proxy servers are recorded, agreed and logged
- filtering issues are eported immediately

- the IT System of the school will be monitored by ensuring:
  - the school IT technical support regularly monitors and records the activity of users on the school IT systems
  - Online Safety incidents are documented on My Concern and reported immediately to the DSL who will arrange for these to be dealt with immediately in accordance with the AUP

Examining electronic devices

Pupils are not usually allowed electronic devices in school; however, there may be occasions where older pupils bring mobile phones to school, for example, if they walk to or from school. These are usually left at the school office for safekeeping and collected at the end of the school day.
School staff have the specific power, under the Education and Inspections Act 2006 (and 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.

When deciding whether there is a good reason to examine or erase data or files on a 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 Deputies, to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or breach of school discipline), and/or
- Report it to the police.

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:
DfE guidance

Data Protection

The school website's Data Protection Policy and Privacy Notices provide full details of the requirements that need to be met in relation to the Data Protection Act 2018.

The school will:

- at all times take care to ensure the safe-keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- store or transfer data using approved services such as remote access, encryption and secure password protected devices
- make sure data is deleted from the device once it has been transferred or its use is complete

- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection officer (Paul Stratford)
- check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely.

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers and to provide information about the school on the website. The school will:

- when using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images both on school devices and personal devices where permission has been given by the Head Teacher
- make sure that images or videos that include pupils will be selected carefully with their knowledge
- seek permission from parents or carers before images or videos of pupils are electronically published
- encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission
- help all parties to recognise that any published image could be reused and repurposed
- make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance
- not publish pupils' work without their permission and the permission of their parents
- keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use

Communication (including use of Social Media)

A wide range of communications' technologies have the potential to enhance learning. The school will:

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure email system
- ensure that any digital communication between staff and parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- use email at Key Stage 1 through a group or class activity with an adult sending and opening emails
- provide pupils at Key Stage 2 with monitored individual school email addresses
- teach pupils about email safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this required

with respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school
- control access to social media and social networking sites in school

- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences
- provide staff with the tools to risk assess sites before use and check the site's terms and conditions to ensure whether the site is age appropriate and whether content can be shared by the site or others without additional consent being given
- make sure that staff official blogs will be password protected (via the school website) with approval from the Senior Leadership Team
- ensure that any digital communication between staff and parents/carers is open, transparent and professional in tone and content
- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe, professional behaviour in line with our staff code of conduct
- advise staff that no reference should be made to pupils, parents/carers or school staff
- advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- register concerns regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- support staff to deal with the consequences of hurtful or defamatory posts about them
- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the SLT

with respect to mobile phones

- inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils', unless they have the permission of the Head Teacher
- inform staff that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team
- inform all that personal devices should be password protected
- advise staff not to use their personal mobile phone to contact parents/carers or pupils
- provide a mobile phone for activities that require them (e.g. school trips)
- inform visitors of the school's expectations regarding the use of mobile phones
- if pupils are allowed to bring mobile phones into school, e.g. if walking to school in Year 6, ensure phones are left in the office during the school day and collected at home time
- maintain the right to collect and examine **any** phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school internet connection

with respect to other personal devices

- **discourage** pupils from bringing their own devices to school, unless by prior arrangement and to support planned learning experiences
- ensure that, if pupils are using their own device (as above, by prior arrangement), they sign an addition to the pupil AUP to agree to responsible use
- ensure that staff understand that the AUP will apply to the use of their own portable devices for school purposes
- Wherever possible, enable the use of the school's Wi-Fi while on the school site
- inform all that personal devices should be charged prior to bringing it to school, so that they are not accidentally placed with school devices
- maintain the right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school internet connection.

In order to avoid any confusion for pupils, staff need to be very clear on the purpose of allowing any use of personal devices in school.

Any agreement allowing pupils to bring devices to school for a planned learning experience MUST be seen by the Head Teacher in advance.

The following table shows how the school considers the way these methods of communication should be used.

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed in consultation with DSL	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones or other camera devices			X			X		
Use of personal devices		X				X		
Use of personal email in school, or on school network		X						
Use of school email for personal emails				X				X
Use of chat rooms / facilities				X				X
Use of messaging apps				X				X
Use of social networking sites, including Twitter			X					x
Use of blogs			X				X	
Use of video broadcasting e.g. YouTube	x						X	

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor West Northants Council can accept liability for the material accessed or consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of child abuse then the monitoring will be halted and referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- The member of staff will record all reported incidents and actions taken and report this to the Head Teacher
- The Designated Safeguarding Lead will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage Online Safety incidents in accordance with the School Behaviour Policy where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact MASH and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO) or advice sought from the MASH team on 0300 126 1000.

The police will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation):

- child sexual abuse images
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity including radicalisation and terrorism

- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

In addition, the following indicates school policy on these uses of the internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)		X		
Online gaming (non-educational)				X
Online gambling				X
Online shopping / commerce			X (i.e. school ordering)	X (i.e. personal)
File sharing (using p2p networks)			X	

Sanctions: Pupils

Incidents	To be dealt with by			Consequence in line with behaviour policy – issued a senior leader only after consideration of the facts			Who else will be involved (depending on the severity of the incident, including age/stage of pupil)		
	Class teacher	Refer to Key Stage Lead	Refer to Deputy or Head	3 or warning	Yellow Card	Red Card	Parents/carers	Technical support (e.g. filtering)	Police
Deliberately accessing or trying to access material that could be considered illegal			X			X	X	X	X
Unauthorised use of non-educational sites during lessons	X			X			X	X	
Unauthorised use of personal device		X			X		X		
Unauthorised use of social networking / instant messaging / personal email			X	X			X	X	
Unauthorised downloading or uploading of files		X			X		X	X	
Allowing others to access school network by sharing username and passwords		X			X		X	X	
Attempting to access or accessing the school network, using another pupil's account			X			X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff			X			X	X	X	
Corrupting or destroying the data of other users		X				X	X	X	
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature			X			X	X		
Continued infringements of the above, following previous warnings or sanctions			X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X	X		
Using proxy sites or other means to subvert the school's filtering system			X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		X	X	
Deliberately accessing or trying to access offensive, pornographic or extremist material			X			X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X		
			NB: Please refer to our Behaviour Policy for more information regarding consequences.						

Sanctions: Staff

	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff for action, eg filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).				L,P			X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X				X		
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X				X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection or network security rules		X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		X				X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners		X	X	L				X
Breech of the school Online Safety policies in relation to communication with learners		X	X	L				X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils		X	X	L			X	X
Actions which could compromise the staff member's professional standing		X	X				X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					X
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X		L	X			
Deliberately accessing or trying to access material which is offensive, pornographic,or seeks to radicalise		X		L			X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X	X			X	X

USEFUL WEBSITES AND LINKS

https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/bullying-social-networks/

https://staysafeonline.org/get-involved/at-home/gaming/

https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/

https://www.childnet.com/resources

LINKS WITH OTHER POLICIES

This policy is linked our:

- Child Protection and Safeguarding Policy
- Behaviour Policy (specifically: consequences, including yellow & red cards)
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Policy