ASTON FIELDS MIDDLE SCHOOL

Online Safety/ACCEPTABLE USE POLICY

Date: **September 2024**

Reviewed: **Annually in September**

Aston Fields Middle School
Online Safety/Acceptable Use Policy

Introduction

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

Staff in schools, as well as children and young people, may be affected by online safety issues including cyberbullying and sexting incidents. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. Dealing with incidents quickly and effectively is key to minimising harm in potentially highly stressful situations. Online safety, however, is about more than cyberbullying. It is about protecting one's online reputation, the managing of personal information and the responsible use of technologies, including social media.

Staff in school are aware that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as defined in KCSIE (2023):

- **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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying)

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

School will ensure online safety is addressed throughout the curriculum and is reflected as required in all relevant policies alongside the Safeguarding and Child Protection policy.

Roles and Responsibilities

Governors

The Governing Body will ensure that comprehensive Online Safety education is provided which includes support for both pupils and staff on managing personal information in on-line environments, and in using personal and social technologies responsibly.

Headteacher and Senior Leaders

The Headteacher and Senior Leaders will ensure that the school has a nominated person as Online Safety Lead tasked with overseeing and managing the recording, investigation and resolution of Online safety incidents. This is Mrs H Mynott, Designated Safeguarding Lead. The DSL will work with the responsible governor and IT service providers in all aspects of filtering and monitoring.

IT Manager/Technical Staff

The IT manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy

- the Filtering and Monitoring procedures are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person whilst overseen by the DSL
- that monitoring software / systems are implemented and updated as agreed in school policies and in accordance to KCSIE 2023

Teaching and Support Staff

Are responsible for ensuring:

- they have an up to date awareness of online safety matters and of the current school Online Safety/Acceptable Use policy and practices
- they know how to report online safety concerns according to the school's safeguarding procedures
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they understand and apply the school's filtering and monitoring arrangements

Designated Safeguarding Lead

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the Safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- Attend relevant governing body meetings/groups
- Report regularly to Headteacher/Senior Leadership Team
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

Pupils

Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They will:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to 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 policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety/Acceptable Use Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents and carers will be encouraged to support the school in promoting good online safety practice including through discussion and reading of online safety advice and guidance through newsletters, fact sheets and the online safety pages on the school website.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims using school issued devices, but must follow school policies concerning the sharing, distribution and publication of those images. Except in exceptional circumstances and with the express permission of the Headteacher or the Designated Safeguarding Lead, those images should only be taken on or saved on school equipment. The personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Filtering and Monitoring
The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is reviewed on a regular basis and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.
Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor. In particular, when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. SWGfL Test filtering.

Filtering
- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)

If necessary, the school will seek advice from, and report issues to the SWGfL Report Harmful Content site.

Monitoring
The school has monitoring systems in place to protect the school, systems and users:
- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by a member of staff or the Designated Safeguarded Lead when necessary. All users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

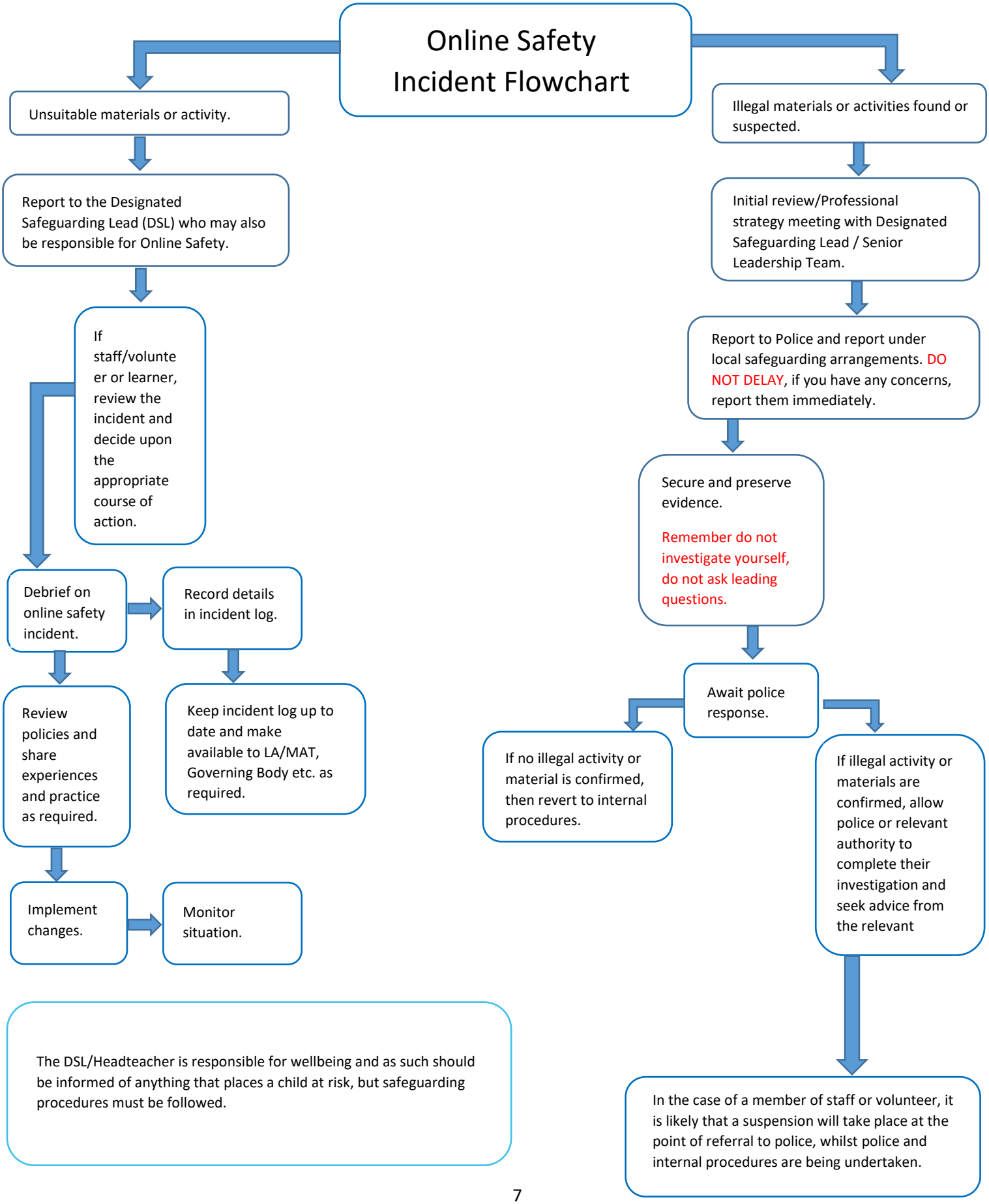
Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not 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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing	X				
Use of social media			Staff		
Use of messaging apps			Staff		
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse – flow chart



Aston Fields Middle School

Acceptable Use Agreement - community user

As a member of our school staff, you will be able to make use of our school's IT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- **I understand that the school will monitor my use of the IT systems, email and other digital commuenications.**
- I will not disclose my username or password to anyone else; nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school/academy's staff.

I will be responsible in my communications and actions when using the school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical material, adult pornography covered by the Obscene Publications Act copyright material) or any inappropriate material that may cause harm or distress to others.
- I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials described above.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I alter computer settings, except with the specific approval of the school through the IT Manager and SLT.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened to the IT Manager.

I have read and understand the above and agree to use the school IT systems (both in and out of the school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's IT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community User Name:	
Signature:	
Date:	

Social Networking Teacher Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.
- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.
- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.
- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.
- Do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.
- 'Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.
- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary actionand possible failure to gain employment in the future.
- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause frictionin your school and make your working environment uncomfortable.
- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.
- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform a member of SLT. Further advice to help with cyberbullying incidents etc. can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.I understand that Injudicious me of social networking may lead to disciplinary action. I agree to take all possible precautions as outlined above.

Community User Name:	
Signature:	
Date:	

Aston Fields Middle School

This policy is reproduced in pupils' planners and should be signed by parents/carers and pupils, within 2 weeks of starting the new academic year.

ACCEPTABLE USE POLICY

(Please read the following with your child and sign the appropriate box on the next page, before returning to school to show your teacher)

The following rules of conduct apply to the use of IT in and for school purposes.

Assessing and using unsuitable images and language

The school wishes to protect the young people in its care from swearing, violent, racist, sexual or similar offensive and age-inappropriate language and images. For this reason the school has internet filters and also monitor your use of IT within the school and outside of school when you are logged on with your school username. Everything you do or access can be made available to your teachers and parents/carers.

Rules

- **I will only use school IT systems, including the internet, email, digital video, mobile technologies etc, for school purposes**
- **I will not write things that would be considered unacceptable in a classroom**
- **I will not try to bypass the internet filtering system**
- **I will not deliberately browse, download, upload or send material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher**

Bullying, harassment and illegal activities

The school wants all pupils and staff to have positive and friendly relationships. It is also important that we ensure you do not use our IT systems to break any laws or plan to break any laws. This includes respecting copyright trademarks.

Rules

- **I will make sure that all IT communications with pupils, teachers or others are responsible and sensible**
- **I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute**
- **I will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or texts that could upset or offend any member of the school community**
- **I will not make illegal copies of copyrighted software, music, images or texts**

Privacy

The content of the school IT systems is only available to be viewed by people connected to our school. Sometimes you may contribute to projects which are viewable by all schools in Worcestershire and sometimes you may work with other schools outside of the country. It is important that you do not copy or move content to places that would infringe another user's privacy. This is to keep you and other users safe.

Rules

- **I will not give out any personal information such as name, phone number or address**
- **I will not arrange to meet someone unless this is part of a school project approved by my teacher**
- **I will respect the privacy and ownership of others' work on-line at all times**
- **I will not download, copy or distribute any pictures, videos, names, text or other content on learning platforms unless I have specific permission**

Username and Password

Everything that you do whilst logged on is monitored and can be traced back to your username. Also, when using forums and messaging, it is important that other people know they are actually communicating with you when they see your username being used.

Rules

- **I will only log on to the school network with my own username and password**
- **I will follow the school's IT securing system and not reveal my passwords to anyone including my friend and parents/carers**
- **I will not allow anyone to use a computer or website that has been logged on with my username unless told to by my teacher**
- **I will tell the school as soon as possible of any unauthorised use of my username, password, other account information or any other breach of security that I become aware of**

Viruses, physical and cyber attacks

You must help the school defend itself against viruses and cyber-attacks as well as misuse of the equipment.

Rules

- **I will not download any software or application on to school computers**
- **I will not do anything that will damage the school IT systems or the ability of others to use them**
- **I will not repeatedly send messages just to make it difficult for someone to work**
- **I will not change the configuration, cabling or monitor/keyboard setting of a computer in a way that will make it difficult for others to use**
- **I will not bring in a memory stick with files on it to use on the school network**

Using technology and social media responsibly

Everyone has a right to use the internet safely both in and out of school. Your actions when using your phone/i-pad/game station **are your responsibility.** You will be taught and encouraged to use technology and social media responsibly in your IT lessons.

Rules

- **I will not upload or send inappropriate photographs or images to any social networking sites that would harm myself or someone else associated with my school**
- **I will not make comments that are thoughtless or hurtful on a social media or gaming site that could lead to accusations of bullying in school**
- **I will tell my partner/carer or an adult I trust if someone else has behaved irresponsibly and put me in danger or made me feel uncomfortable**

Consequences of breaking the rules

The rules are designed to keep you and other users safe and the school will enforce the rules using the normal range of sanctions, including contacting parents/carers and involving the police if necessary. We may also ban children from using part of our IT systems for a period of time decided by the Headteacher or Deputy Headteacher.

Where we consider it appropriate, we may also pass on information about you or what you have been doing on the school IT systems or on your own devices, out of school, to the police, courts or other people. We will do this if we believe it will help us to enforce our rules to protect the safety of people or property.

Please sign and show your Class Teacher for signature by mid-September

Acceptable Use Policy (academic year inserted)

We have read and agree to abide by the rules and code of conduct outlined for safe use of IT for school purposes.

Pupil ……. Class ……

Parent/Carer …….. Date ……

The Online Safety/Acceptable Use Policy will be reviewed annually.

ACCEPTABLE USE POLICY

(Please read the following with your child and sign the appropriate box on the next page, before returning to school)

The following rules of conduct apply to the use of ICT in and for school purposes.

Accessing and using unsuitable images and language
The school wishes to protect the young people in its care from swearing, violent, racist, sexual or similar offensive and age-inappropriate language and images. For this reason the school has internet filters and also monitors your use of ICT within the school and outside of school when you are logged on with your school username. Everything you do or access can be made available to your teachers and parents/carers.

Rules:

- **I will only use school ICT systems, including the internet, email, digital video, mobile technologies, etc. for school purposes.**
- **I will not write things that would be considered unacceptable in a classroom.**
- **I will not try to bypass the internet filtering system.**
- **I will not deliberately browse, download, upload or send material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.**

Bullying, harassment and illegal activities
The school wants all pupils and staff to have positive and friendly relationships. It is also important that we ensure you do not use our ICT systems to break any laws or plan to break any laws. This includes respecting copyright trademarks.

Rules:

- **I will make sure that all ICT communications with pupils, teachers or others are responsible and sensible.**
- **I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.**
- **I will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.**
- **I will not make illegal copies of copyrighted software, music, images or texts.**

Privacy
The content of the school ICT systems is only available to be viewed by people connected to our school. Sometimes you may contribute to projects which are viewable by all schools in Worcestershire and sometimes you may work with other schools outside of the county. It is important that you do not copy or move content to places that would infringe another user's privacy. This is to keep you and other users safe.

Rules:

- **I will not give out any personal information such as name, phone number or address.**
- **I will not arrange to meet someone unless this is part of a school project approved by my teacher.**
- **I will respect the privacy and ownership of others' work on-line at all times.**
- **I will not download, copy or distribute any pictures, videos, names, text or other content on learning platforms unless I have specific permission**

Username and password
Everything that you do whilst logged on is monitored and can be traced back to your username. Also, when using forums and messaging, it is important that other people know they are actually communicating with you when they see your username being used.

Rules:

- **I will only log on to the school network with my own username and password.**

ACCEPTABLE USE POLICY

Rules

- **I will only log on to the school network with my own username and password**
- **I will follow the school's IT securing system and not reveal my passwords to anyone including my friend and parents/carers**
- **I will not allow anyone to use a computer or website that has been logged on with my username unless told to by my teacher**
- **I will tell the school as soon as possible of any unauthorised use of my username, password, other account information or any other breach of security that I become aware of**

Viruses, physical and cyber attacks
You must help the school defend itself against viruses and cyber-attacks as well as misuse of the equipment.

Rules

- **I will not download any software or application on to school computers**
- **I will not do anything that will damage the school IT systems or the ability of others to use them**
- **I will not repeatedly send messages just to make it difficult for someone to work**
- **I will not change the configuration, cabling or monitor/keyboard setting of a computer in a way that will make it difficult for others to use**
- **I will not bring in a memory stick with files on it to use on the school network**

Using technology and social media responsibly
Everyone has a right to use the internet safely both in and out of school. Your actions when using your phone/i-pad/game station **are your responsibility.** You will be taught and encouraged to use technology and social media responsibly in your IT lessons.

Rules

- **I will not upload or send inappropriate photographs or images to any social networking sites that would harm myself or someone else associated with my school**
- **I will not make comments that are thoughtless or hurtful on a social media or gaming site that could lead to accusations of bullying in school**
- **I will tell my partner/carer or an adult I trust if someone else has behaved irresponsibly and put me in danger or made me feel uncomfortable**

Consequences of breaking the rules
The rules are designed to keep you and other users safe and the school will enforce the rules using the normal range of sanctions, including contacting parents/carers and involving the police if necessary. We may also ban children from using part of our IT systems for a period of time decided by the Executive Leader/Headteacher/ National Leader of Education or Heads of School/Acting Headteachers.

Where we consider it appropriate, we may also pass on information about you or what you have been doing on the school IT systems or on your own devices, out of school, to the police, courts or other people. We will do this if we believe it will help us to enforce our rules to protect the safety of people or property.

Please sign and show your Class Teacher for signature by mid-September

Acceptable Use Policy (2023-2024)

We have read and agree to abide by the rules and code of conduct outlined for safe use of IT for school purposes.