# SRS Online Safety Policy

| | |
|---|---|
| Lead Governor | Curriculum |
| Updated | September 2025 |
| Adopted | September 2025 |

Headteacher: Miss Zoë Baines
SLATED ROW SCHOOL | THE ASPIRE FEDERATION, MILTON KEYNES

# Contents

# 1. Aims

Our School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others, understanding that all students at Slated Row School have increased vulnerability due to their SEND needs
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

This policy is adapted from the Key for School Leaders and is based on the Department for Education's (DfE) 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.

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 cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on Students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

# 3. Roles and responsibilities

## 3.1 The Governing Board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is Cathy Mingo.

All governors will:

- Make sure 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 (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure 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

## 3.2 The Headteacher

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

## 3.3 The Designated Safeguarding Lead

- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager 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
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- 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
- Undertaking annual risk assessments that consider and reflect the risks pupils face

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

Note: This list is not intended to be exhaustive.

## 3.4 The ICT Manager

The ICT Manager in each school 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Note: This list is not intended to be exhaustive.

## 3.5 All staff and volunteers

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 (appendix 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting to DSL who will complete the online safety incident log.
- Following the correct procedures, by requesting authorisation from the Headteacher, if they need to bypass the filtering and monitoring systems for educational purposes

- Working with the DSL to ensure that any online safety incidents are logged 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 will happen here'

Note: This list is not intended to be exhaustive.

## 3.6 Parents/Carers

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 (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent fact sheet - Childnet International

## 3.7 Visitors and members of the community

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 and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

# 4. Educating Students about online safety

Pupils will be taught about online safety as part of the curriculum

Guidance is taken from both the National Curriculum computing programmes of study and guidance on relationships education, relationships and sex education (RSE) and health education.

In **Key Stage 1**, Students will be taught to:

- Use links to websites to find information.
- Recognise age appropriate websites.
- Use safe search filters.
- Understands and follows rules around using technologies and equipment.

- Knows to tell someone if something upsets them online.
- Understands that not everyone who makes contact online is safe.

- Understand that they do not need to do something which may make them unsafe.
- Know what to do if they feel unsafe or worried for themselves or others

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

- Describe the world wide web as part of the internet that contains websites.
- Add websites to a favourites list.
- Use search tools to find and use an appropriate website and content.
- Understands what is appropriate and who to tell if something/someone is inappropriate.
- Understands how to be appropriate and respectful, when using technologies and the internet.
- Understands what is private information.
- Understands that people are not always who they claim to be online.
- Knows ways of keeping safe online, such as using passwords or having adult help to access the internet.
- Understand the role of the internet in everyday life.
- Knows the common uses of IT beyond school.

- Understand that rules and age restrictions keep us safe.
- Know how to respond safely to adults they don't know.
- Understand the importance of not keeping adults' secrets.
- Understand and demonstrate basic techniques for resisting pressure to do something they don't want to do and which may make them unsafe.
- Know who to ask for help and vocabulary to use when feeling unsafe or worried for themselves or others; importance of keeping trying until they are heard.

In **Key Stage 3**, students will have been taught and will continue to be reinforced:

- Search for information using appropriate websites and advanced search functions within Google.
- Use strategies to check the reliability of information (cross check with another source).
- Understands what is appropriate and how to report concerns and how to respond
- Knows the importance of keeping private information private
- Understands when websites are not legitimate and cannot be trusted.
- Understand the ways in which the internet and social media can be used both positively and negatively.
- Understands how what is posted online might affect ourselves or others and know strategies to help stop and think.
- Understand basic rules for using social media, including age restrictions and why they exist.

- Understand the impact of bullying, including offline and online, and the consequences of hurtful behaviour.
- Know and demonstrate strategies to respond to hurtful behaviour experienced or witnessed, offline and online; how to report concerns and get support.
- Understand about privacy and personal boundaries; what is appropriate in friendships and wider relationships.
- Know how to respond safely & appropriately to adults they may encounter who they do not know.
- Understand about seeking and giving permission (consent) in different situations.
- Understand about keeping something confidential or secret & when it is right to tell someone.
- Know how to recognise pressure from others to do something unsafe or that makes them feel uncomfortable and strategies for managing this.

- Know where to get advice and report concerns if worried about their own or someone else's personal safety.

Students in **Key Stage 4** will be taught and will continue to be reinforced:

- Know how to pay attention to trustworthiness of websites and sources when accessing information online
- Can recognise inappropriate content, contact and conduct online and knows how to report all concerns.
- Recognises the importance of online security, including protecting their online identity and privacy settings.
- Can evaluate how the internet and social media impacts, on both individuals and society at large, both positively and negatively.
- Understands how to use digital resources, including online, respectfully and responsibly.

- Understand the impact that media and social media can have on how people think about themselves and express themselves, including regarding body image, physical and mental health.
- To know how to identify and reduce risk and manage personal safety in increasingly independent situations, including online.
- To know how to manage the breakdown of a relationship (including its digital legacy), loss and change in relationships.
- To recognise peer influence can generate feelings of pressure and to develop strategies for managing it, including online.
- To know the characteristics of abusive behaviours, such as grooming, sexual harassment, sexual and emotional abuse, violence and exploitation; to recognise warning signs, including online; how to report abusive behaviours or access support for themselves or others.
- To recognise bullying, and its impact, in all its forms; the skills and strategies to manage being targeted or witnessing others being bullied.
- To identify the indicators of positive, healthy relationships and unhealthy relationships, including online.
- To recognise how the media portrays relationships and the portrayal of sex in the media and social media (including pornography); and the potential impact of this on people's expectations of relationships and sex.
- To understand the impact of sharing sexual images of others without consent; and how to manage any request or pressure to share an image of themselves or others, and how to get help.

By the end of **Year 14**, students will know:

- Protect personal information and privacy.
- Understand the personal rights and options for controlling the use of personal data.
- Know how to protect devices and data from online risks and threats.
- Know the advantages of backing up data locally and to the Cloud
- Use appropriate language online.
- Know about appropriate behaviour online.
- Know how to apply simple methods to avoid health risks while using devices.
- Know how to apply simple methods to avoid psychological health risks while using devices.

- Understand the ways in which industries and advertising can influence health and harmful behaviours.
- To know ways to identify risk and manage personal safety in new social settings, workplaces, and environments, including online.

- To know strategies for identifying risky and emergency situations, including online; ways to manage these and get appropriate help, including where there may be legal consequences (e.g. drugs and alcohol, violent crime and gangs).
- To know how to recognise unwanted attention (such as harassment and stalking including online), ways to respond and how to seek help.
- To recognise bullying, and its impact, in all its forms; the skills and strategies to manage being targeted or witnessing others being bullied.
- To know how to evaluate ways in which their behaviours may influence their peers, positively and negatively, including online, and in situations involving weapons or gangs.
- To know the opportunities and potential risks of establishing and conducting relationships online, and strategies to manage the risks.
- To understand the legal and ethical responsibilities people have in relation to online aspects of relationships.
- To understand the potential impact of the portrayal of sex in pornography and other media, including on sexual attitudes, expectations and behaviours.

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.

# 5. Educating parents/carers about online safety

Each school will raise parents/carers' awareness of internet safety in letters or other communications to home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Designated Safeguarding Lead.

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

# 6. Cyber-bullying

## 6.1 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. (See also the school behaviour policy.)

## 6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 students, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

## 6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher as set out in the school's behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Headteacher or DSL.
- Explain to the students why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The Student and/or the parent/carer refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

## 6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully students in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

# 7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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.

We will monitor the websites visited by students/carers, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

# 8. Students using mobile devices in school

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2) and the Aspire Federation's Mobile Phone Policy.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Slated Row School recognises that there are times when student's personal devices may be needed (E.g. as a communication device). If this occurs, it should only happen with permission of the Headteacher and a waiver must be completed beforehand by the parents or legal guardian of that student. The link to the waiver is found below and must be completed before the device comes into school. It is also included as Appendix C.

Personal Devise permission form

# 9. 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
- Keeping operating systems up to date – always install the latest updates when prompted

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

# 10. How the school will respond to issues of misuse

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

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 in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

# 11. Training

## 11.1 Staff, governors and volunteers

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.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

  Abusive, threatening, harassing and misogynistic messages

  Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

  Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

# 12. Monitoring arrangements

Each DSL logs behaviour and safeguarding issues related to online safety. These logs should be recorded on CPOMS.

This policy will be reviewed every year by the Headteacher with each school's DSL. At every review, the policy will be shared with the governing board.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Remote learning policy

# Appendix 1: Student acceptable use agreement

# (Students & Parents/Carers)

| Acceptable use of the school's ICT systems & internet: agreement for Students & parents/carers | |
|---|---|
| **Name of Student :** | **Class:** |
| **Name of the person completing the form:** | **Relation to the student:** |

- ☐ I will only use equipment with staff permission.
- ☐ I will only use my own login to access my own and shared files.
- ☐ I will not share my passwords with any other students.
- ☐ I will check copyright before using any files, images or sound.
- ☐ I will use my email account responsibly.
- ☐ I will not put any personal information on Internet sites.
- ☐ To help protect myself and others, I will tell staff if I see anything that bothers me.
- ☐ I understand that the school may check my files and monitor any Internet sites that I visit.
- ☐ I will be kind to others and not upset or be rude to them
- ☐ Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- ☐ Only use websites that a teacher or adult has told me or allowed me to use
- ☐ Tell my teacher or an adult immediately if I click on a website by mistake
- ☐ Tell my teacher or an adult immediately if I receive messages from people I don't know
- ☐ I will not use my school email account to open private accounts on other services (Apple ID for example)

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

| Student Signature: | Date: |
|---|---|

**Parent/Carer's agreement**: *I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for Students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.*

| Parent/Carer Signature: | Date: |
|---|---|

# Appendix 2: Acceptable use agreement (Staff, Governors, Volunteers & visitors)

| Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors | |
|---|---|
| Name: | Staff, Governor, Volunteer or Visitor: |

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of Students without checking the photograph permission sheet held by the Main Office.
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

☐ I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

☐ I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

☐ I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

☐ I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

☐ I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.

| Signed: | Dated: |
|---|---|

# Appendix 3: Student Personal Device Usage (Waiver)

Dear Parent/Carer,
**Personal Device Permission**

If a student has a need to bring a phone / personal device to school, their parent/carer must complete this permission form and return to school.
Please make sure that your child understands the school rules about mobile phone / personal device use. These are very important and are in place to protect all of our students.

- Phones / Personal devices must be turned off at all times on school premises.
- Students must hand their phone / personal device into the school office when they arrive at school.
- The school accepts no responsibility for loss or damage to Mobile Phones/ Personal device
- Students' phones / personal device / personal device should be clearly marked with their name.
- If a student is found to be using a phone / personal device on school premises, this is a serious matter and will be dealt with in accordance with the school's Behaviour Policy.

Schools are permitted to confiscate phones from students under sections 91 & 94 of the Education & Inspections Act 2006.

Please remember that mobile phones / personal devices provide easy access to the Internet which is full of fantastic opportunities but can also be a very risky place. It is important that we all work together to keep children safe. We strongly recommend that you enable parental controls on your child's phone / personal device, and talk to your child about how to stay safe online.

**To be completed by the person with parental responsibility:**

I wish for my child…….
class…… to bring their mobile phone / personal device into school. I understand that it needs to be handed in at the beginning of the day and switched off whilst on the school premises.

**I understand that Mobile phones / Personal devices are brought into school entirely at the owner's risk. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones.**

I also understand that should my child misuse their phone, the school will withdraw permission for them to bring it in and I will be expected to collect the phone / personal device from school myself.

| | |
|---|---|
| Parent signature: | Print Name: |
| Date: | |