St Anne's Catholic Primary School	**Policy Document** **Online Safety Policy**	Last Reviewed: September 2024 Next Review: Sept 2026

School Mission Statement

Our Mission at St. Anne's is to Live, Love and Learn together with Christ.

Statement of intent

At St Anne's we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. **Legal framework**

This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006

- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

This policy also has regard to the following statutory guidance:

DfE (2025) 'Keeping children safe in education':
Keeping Children Safe in Education 2025
St Anne's Safeguarding and child protection policy:
Safeguarding and Child Protection Policy

2.Use of the internet

2.1 The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2 Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- **Online** bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

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 governor who oversees online safety is Mrs Natalie McCleary All governors will:

- Ensure that they have read and understand this policy
- Ensure they have had training on a regular basis about online safety

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, keeping up to date with current legislation and that this policy is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

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

The Designated Safeguarding lead for school is Mrs Patricia Johnston , headteacher.

Deputy DSL's in school are Miss Emily Keedwell and Mrs Alison Turley

The DSL/ Deputy takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of online bullying are logged and dealt with appropriately in line with the school behaviour policy
- 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
- Ensuring filtering and monitoring is in place on school owned devices and regularly testing this

This list is not intended to be exhaustive.

3.4 The ICT manager/leader – Mrs McCabe

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school and on school devices, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 2) ,staff code of conduct and teaching standards, and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of online safety incidents are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents 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 (appendix 1)
- Parents 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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

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 2).

4. Educating pupils about online safety

4.1 Online safety is now a statutory part of the programme of study for all pupils. Rules and technical solutions are not infallible and we are aware that outside school, children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks.

Pupils are taught about online safety in every year group, using a planned progressive online safety curriculum on Project Evolve, based on the DfE guidance document published in June 2020 'Education for a Connected World.' It is provided as part of Computing (through Purple Mash) / RSE (through PHSE lessons) and is regularly revisited throughout the year. Covering the key strands of:

- Online Relationships
- Online Bullying
- Self-Image and Identity
- Online Reputation
- Managing Online Information
- Health, Well-being and Lifestyle
- Privacy and Security
- Copyright and Ownership

Additionally, all schools have to teach the following elements alongside the current guidance:

Relationships education and health and education in primary schools

Pupils in Key Stage 2 will be taught to:

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

By the end of primary school, pupils will know:

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

The safe use of social media and internet will also be covered in other subjects where relevant. Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Teachers and staff use Twitter to model the safe use of social media, this may take place on a school or personal device, please refer to the school social media policy contained within this document at paragraph 13.

Where pupils undertake searching of the internet, staff encourage children to use child friendly search engines e.g Swiggle and monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches, this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

The school will use assemblies and events, such as ‘Safer Internet Day’, to raise pupils’ awareness of dangers that can be encountered online and may also invite trained speakers to talk to pupils about this; where appropriate as a way of enhancing the embedded online safety curriculum.

4.2 Rules for keeping safe

Underpinning the ICT curriculum are the SMART rules, which are reinforced in school across the curriculum:

- **Safe** – encourages young people to be safe by not giving out their personal details online.
- **Meeting** – draws attention to the risks associated with meeting someone you only know online.
- **Accept** – highlights the risks of accepting emails, pictures and text messages from unknown sources.
- **Reliable** – is a reminder that not all information found online is necessarily reliable.
- **Tell** – encourages children to tell someone if something happens or they meet someone online that makes them feel uncomfortable, or if they or someone they know is being bullied online.

These rules are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT and actively monitor device use by users.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety with information via our website. This policy will also be shared with parents.

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

Parents are responsible for pupils' behaviour online at home, school may support parents if an incident involves other pupils at school.

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

6. Online Safety control measures

6.1 Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.
- A record will be kept by the headteacher of all pupils who have been granted internet access.

- Monitoring is outsource to the Local Authority Online monitoring service using two different monitoring solutions in school, Smoothwall Monitor for Networked and Chromebook devices and Securus for iPad monitoring. Smoothwall monitor and Securus both allow the LA service to alert to any incidents and report to the Headteacher.

  Smoothwall Monitor is used across the network in order to

- Monitor inappropriate use of language
- Monitor internet usage Inc. words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy (See Appendix)

Any identified incident is reported to Mrs Johnston, in order for it to be investigated and dealt with. Incidents of every level are also monitored and reported by the Local authority online safety advisor and reported via email.

A weekly report that is a reassurance email is sent from Smoothwall that gives an update on the number of users (people who log into devices), the number of devices that are being monitored and number of captures in the week. A monthly report is sent that includes details relating to school captures and incidents. This helps and supports us to identify the risk profile and look at patterns in the captures.
The monitoring software does not negate the need for staff to supervise pupils when using devices. iPad use should be fully supervised by staff and websites given to pupils in order to reduce the risk of coming across inappropriate content. iPads are allocated to pupils, e.g. iPads numbered, and children allocated to a number, so that staff know which child is on which device when incidents do occur as these may be reported some time after the incident has occurred.

- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material. St Anne's use Fortinet to control filtering and this is managed by the Local Authority Schools ICT support on behalf of the school.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- If staff comes across unsuitable on-line materials, the site must be reported immediately to the DSL. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the DSL. Staff are now able to

access sites such as ‘You Tube’ and others on request but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. **Links and content should be checked in school just prior to use in the classroom due to daily rotation of advertising content and ability to access in school.**

  - Staff will check all videos and content before use with pupils

- ___ (who) will ensure that the school’s filtering system is working by randomly checking logins and devices, half termly, using ‘test filtering’ www.testfiltering.com. A screen shot of the checks will be made and saved on the school’s network.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the Online Safety officer for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from using any personal devices. This will be dealt with following the process outlined in section 9.2 of this policy.

The school are currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. This is being implemented by Walsall Council Online Monitoring service by:

- active monitoring and automatic alerts for the school to act upon, together with proactive monitoring by Walsall Council to support the school by drawing attention to concerning behaviours, communications or access
- ability to produce reports on the websites visited by all young people and adults using our systems
- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up
- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff
- automated reporting to ensure that processes are followed without fail

All devices are monitored in school when using devices in school the internet is filtered, pupils are taught about making the correct choices when online and staff should fully and actively supervise pupils during activities.

6.2 Email:

- Staff will be given approved email accounts and are only able to use these accounts.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Staff members are aware that their email messages are not monitored.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

6.3 Social networking:

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

6.4 Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.

- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

6.5 Mobile devices and hand-held computers:

- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use, i.e. Year 6 walking to and from school.
- Pupils are not permitted to access the school’s Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the Online Safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of pupils or staff, with the exception of paragraph 11.2
- The school will be especially alert to instances of online abuse including online bullying and will treat such instances as a matter of high priority.

6.6 Network security:

- Network profiles for staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords have a minimum and maximum length, to prevent ‘easy’ passwords or mistakes when creating passwords.
- Passwords will expire after 90 days to ensure maximum security for staff accounts.

6.7 Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the ICT technician from Walsall LA on behalf of the school.
- The ICT technician will ensure that the filtering of websites and downloads is up-to date and monitored. Computers are up to date with the latest software and support the school with any other online safety issues as required.

7. Dealing with online safety incidents

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and are fully aware of their responsibilities to follow up any reported issues.

Staff should report online safety issues to the DSL via CPOMS. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the Headteacher or to the Chair of Governors, if the headteacher is absent or the accusation involves the headteacher this should go to the LADO via Walsall MASH 0300 555 2866.

Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend.

We encourage children to take responsibility for protecting each other.

7.1 Managing incidents

In the event of suspicion of an infringement of policy on a school device then all the following steps should happen:

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images including youth produced imagery, nudes and semi nudes, as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may include internal procedures, involvement of LA or police.

8. Acceptable use of the internet in school

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet, (Appendix 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant, when using school devices.

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 on school devices visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendix 1 and 2.

9. Reporting misuse

St Anne's will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

Inappropriate activities are discussed and the reasoning behind prohibiting activities due to Online Safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

9.1 <u>Misuse by pupils</u>:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

9.2 <u>Misuse by staff</u>:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a Complaints Form.
- The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy, and may decide to take disciplinary action against the member of staff.

- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

9.3 <u>Use of illegal material:</u>

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.

10. Pupils using mobile devices in school

- Pupils may bring mobile devices into school, but are not permitted to use them on school premises as the school provides access to technologies which can be used for learning. Mobile devices are handed in at the start of the day and are stored in the office. They are then collected at the end of the day and handed back to pupils.

- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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

11. Staff devices

11.1 <u>Staff using work devices outside of school</u>

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)
- Making sure the device locks if left inactive for a period of time

- The device can be used for personal use but staff are reminded that this is monitored so all staff should be mindful of all activity taking place on it
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

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 2.
If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

11.2 Staff mobile devices in school

Staff are not allowed to use their personal mobile devices including smart watches in school while they are teaching and any use should be restricted to times when children are not present. Mobile devices may be used in staff room or offices where children are not present, but this use should be minimised. The desired option is for phone calls to be made outside of the school building or in the staff room or designated offices. The only exception to this is in case of emergency during a school trip. Staff may wear Smart watches/technology but these should be silenced and notifications not allowed during teaching time and staff should not respond to alerts/notifications.

If Staff use their own mobile device to take images of children, for example on a school trip, staff should download and delete these images immediately. These should not be stored or backed up in anyway, backups should be deleted straight away too.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and 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.

13. Social Media Policy - Internet and Network access from personal devices

13.1 Visitors to school including Governors

Visitors and governors can gain access to Wi-Fi on personal devices. The Wi-Fi is password protected and they will need to ask for the password first. All internet activity is filtered. Any guest/visitor users are given the student internet access where internet is heavily filtered.

13.2 Staff access

Staff can access the school Internet via a school devices and can access the school Wi-Fi on personal devices but should be mindful of what they are doing on devices.

13.3 Communications Technologies

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.

Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.

Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site (Governor Hub) that governors can access to via a personal user account.

Personal email addresses, text messaging, public chat and social networking programmes are not being used for communications with parents/carers and children. Personal information is also not posted on the school website.

13.4 Personal Social Media use

Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.

Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community

Personal opinions are not attributed to the school

Security settings on personal social media profiles are regularly checked to minimise risk Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.

13.5 School Twitter account

The school have a twitter account which is used to communicate about school life, achievements and updates. The headteacher is responsible for the posts on the account. Any incidents of misuse or communication are dealt with in accordance with the acceptable use policies.

14. Use of Digital Images and Videos

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for online bullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupil’s full names are not published on any online platform or school communication including the web site, or newsletter. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils’ full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- 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 this is not covered by the General Data Protection Regulation. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

- Pupils' work is only published with the permission of pupils and parents / carers.

15. Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including online threats 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).
- The DSL 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.

16. Monitoring and review

This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff

Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Appendix One –

Pupil Acceptable use policies EYFS Acceptable Use policy

mini mash
2simple

✓ I tap or click on things I have been shown.

✓ I ask before I use a tablet, computer or camera.

?
WARNING CLICK HERE

✓ I check if I can tap/click on things I haven't seen before.

✓ I tell a grown-up if something upsets me.

My name: ……………………………………

Date: …………………………

KS1 Acceptable use policy

This is how we stay safe when we use computers:

- I will ask a teacher or trusted adult if I want to use the chromebooks/iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or trusted adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use the chromebooks/iPads
- I KNOW people online aren’t always who they say they are
- I don’t keep SECRETS or do DARES AND CHALLENGES just because someone tells me I have to
- I am KIND and polite to everyone

My Name …………………………………………………………………………..

Date: ……………………………………………………………

KS2 Acceptable use policy

- I will only access computing equipment when a trusted adult has given me permission and is present – at home or at school.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform a trusted adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others. I will also make sure my password is strong and difficult to guess.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will be careful with what I click on online I won't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify a trusted adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as Google Classroom. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I will only communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
- I know new online friends might not be who they say they are and I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are and know when to say no online.

Before I share, post or reply to anything online, I will T.H.I.N.K.
T = Is it true?
H = Is it Helpful?
I = Is it Inspiring?
N = Is it Necessary?
K = Is it Kind?

I understand that if I behave negatively whilst using technology towards other members of the school, my family will be informed and appropriate actions taken.

My name: …………………………………………………………………………………………

Date: …………………………

Appendix Two:

STAFF ACCEPTABLE USE POLICY AND AGREEMENT Introduction

This policy is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices. Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Head Teacher/Online safety lead.

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.

Users must not try to install any software on the ICT systems without permission from the Head Teacher/Online safety lead. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Head Teacher/School Business Manager are responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging. Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

Network access and security

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the SLT for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Head Teacher/Online safety lead as soon as possible.

Users should only access areas of the school's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

School Email

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy. The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address. When using our class email to communicate with parents, all emails will be saved. Communication with our families will be professional in tone and manner.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.

- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible. Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.

Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).

Staff will be encouraged to develop an appropriate work life balance when responding to email.

Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

Internet Access

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Head Teacher/Online safety lead.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;

- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;

  transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital cameras

The school encourages the use of digital cameras and video equipment; however, staff should be aware of the following guidelines:

□ Photos should only be named with the pupil’s name if they are to be accessible in school only. Photos for the website or press will not include pupil names without parental consent.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Devices

Mobile devices are permitted in school, with the following restrictions:

They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard.

- All phone contact with parents regarding school issues should be through the schools phones. If personal mobile phones are used, then 'number witheld' must be activated.
- Personal mobile numbers should not be given to parents at the school.

Social networking

In line with the Social Media Policy contained within this policy the key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via the officially recognised school site and with the permission of the Head Teacher or the Deputy Head Teacher.
- Members of staff will notify the Head Teacher/Online safety lead if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.

- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by Smoothwall. SLT and the Online safety lead to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, email and/or social networking site accounts, which the the Head Teacher/Online safety lead considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

STAFF ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a school user of the network resources/ equipment I hereby confirm that **I have read and understood the Acceptable Use Policy** and that I agree to follow the school rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Head Teacher.

I agree to report any misuse of the network to the Head Teacher. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Hed Teacher. I finally agree to ensure that portable equipment such as cameras, ipads or laptops will be kept secured when not in use and to report any lapses in physical security to the Head Teacher.

Specifically when using school devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Signed ………………………………………………… Date ……………….

Print name ………………………………………………………………………