



**St. Philip's**  
RC Primary School

## **E-Safety Policy**

---

**Updated March 2025**

## Introduction

This School E-Safety Policy Template is intended to help school leaders produce a suitable ESafety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti- Bullying policies.

The School E-Safety Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

## Policy Governance

### Development, Monitoring and Review of this Policy

This e-safety policy has been developed by the school's e-safety officer in conjunction with the Headteacher (Miss McNamara)

Position	Name(s)
<i>School E-Safety Coordinator / Officer</i>	Mr J. Cooper
<i>Headteacher</i>	Miss McNamara
<i>Teachers</i>	N/A
<i>Support Staff</i>	Miss Brady (Pastoral care)
<i>ICT Technical staff</i>	Computeam
<i>Governors</i>	Mr. Rafael Martinez (Safeguarding) Mr S. Makuwere
<i>Parents and Carers</i>	Mr. Rafael Martinez and Mr. S. Makuwere
<i>Community users</i>	N/A

## Schedule for Review

This e-safety policy was approved by the	<i>Governing Body:</i>
The implementation of this e-safety policy will be monitored by:	<i>E-Safety Officer Senior Leadership Team</i>
Monitoring will take place at regular intervals:	<i>Annually, in September</i>
The <i>Governing Body / Governors Sub Committee</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group ( <i>or named individual</i> ) at regular intervals:	<i>Annually</i>
The E-Safety Policy will be reviewed <i>annually</i> , or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	<i>Annually, in September</i>
Upon review of the E-Safety Policy, an annual risk assessment review will take place	<i>Annually, in September</i>
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>See Incident Management Section</i>

## Scope of the Policy

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

### Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

#### **Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Governing bodies and proprietors will ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction

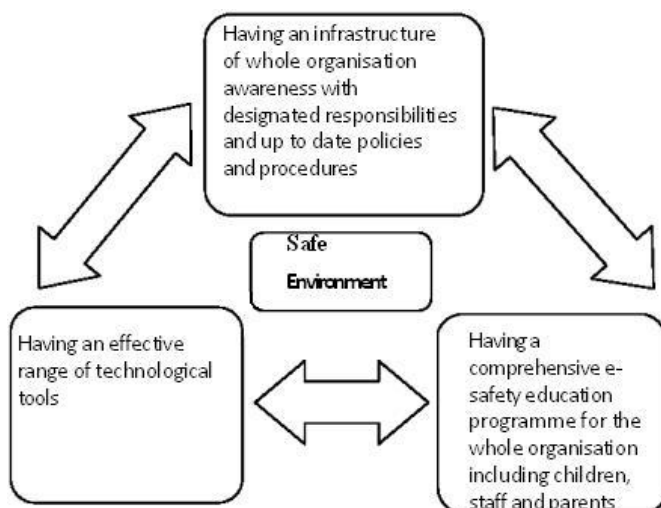
All Governors receive Safeguarding and Child Protection training at induction and continue to attend regular updates that are relevant to their role, including an understanding of the roles and responsibilities in relation to the online filtering and monitoring systems in the school

#### **Headteacher and Senior Leaders:**

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community

The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

Will promote a safe environment by:



Senior Leaders will ensure that:

**Does your organisation.....**

1. Have a nominated e-safety coordinator?
2. Have the necessary acceptable use policies?
3. Check that appropriate e-safety procedures and practices are in place and working?
4. Use an accredited supplier for internet services?
5. Include e-safety as part of your inspection evidence?
6. Keep a log to record and monitor e-safety incidents?
7. Raise awareness of e-safety issues by holding workshops and events?

**Do all your staff and volunteers.....**

1. Understand e-safety issues and risks?
2. Receive regular training and updates?
3. Know how to support youngsters with new technologies?
4. Know how to report and manage issues or concerns?
5. Know how to keep data safe and secure?
6. Know how to protect and conduct themselves professionally online?
7. Take the opportunity to consult with children and young people?

**Do your children and young people.....**

1. Understand what safe and responsible online behaviour means?
2. Get opportunities to learn about e-safety?
3. Get the opportunity to improve their digital literacy skills, e.g. how to search safely and effectively online?
4. Know the **SMART** (Safe, Meeting, Accepting, Reliable, Tell) rules?
5. Get the opportunity to give their views about staying safe online?
6. Know how to report any concerns they may have?

**Can your parents and carers.....**

1. Understand e-safety issues and how to manage risk?
2. Understand their roles and responsibilities?
3. Receive regular training and updates?
4. Understand how to protect their children in the home?

**E-Safety Coordinator/Officer:**

Leads the e-safety committee and/or cross-school initiative on e-safety

Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents

ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

provides training and advice for staff

receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

reports regularly to Senior Leadership Team

### **Network Manager / Technical staff:**

From April 2021, Computeam will provide technical curriculum support utilising Salford's broadband and filtering. From July 2021, broadband and filtering will be provided by Computeam through a leased line. The School's SIMS management information system will continue to be supported by RM and hosted remotely by Salford City Council.

CompuTEAM will ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack. This will be ensured by maintaining a robust firewall system which protects all users from malicious, dangerous or inappropriate content.

That the school meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance

That users may only access the school's networks through a properly enforced password protection policy

The school uses two safeguarding products: Securly Filter and Securly Aware.

The Securly Filter is a cloud based filtering solution that monitors and blocks web based content for the school users. With it being cloud based it works on school devices even if they are not on the premises. It generates a weekly report for the prevent duty. This report shows content which users have tried to access and has AI built in to remove any false positives. The system is setup for live alerts allowing the DSL to deal with issues immediately before the report is generated.

The reports are sent to the following designated leads on the Securly system:

- [Amanda.Mannion@stphilipsrcprimary.com](mailto:Amanda.Mannion@stphilipsrcprimary.com)
- [Catherine.Lavelle@stphilipsrcprimary.com](mailto:Catherine.Lavelle@stphilipsrcprimary.com)
- [Ruth.McNamara@stphilipsrcprimary.com](mailto:Ruth.McNamara@stphilipsrcprimary.com)
- [John.Cooper@stphilipsrcprimary.com](mailto:John.Cooper@stphilipsrcprimary.com)

### **Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school esafety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the appropriate person, as defined in *Section 11*

Designated person for child protection/Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child Protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- E-Safety Committee

Members of the E-safety Committee (this includes the Headteacher, Safeguarding Committee, Link Governor, Chair of Governors and key members from partnership schools) will assist the E-Safety Coordinator/Officer with:

- The production, review and monitoring of the school e-safety policy

### **Students/pupils:**

- Are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. In KS1, parents would sign on behalf of pupils; in KS2, pupils do this independently.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

### **Parents/Carers:**

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy
- Accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

### **Community Users**

Not applicable at St. Philip's.

### **E-Safety Education and Training**

Education – students / pupils

E-Safety education will be provided in the following ways:

A planned e-safety programme will be provided as part of Computing lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school

Key e-safety messages will be reinforced as part of a planned programme of assemblies.

Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

E-safety rules will be displayed in all classrooms.

A prominent display will be produced to remind pupils of the key messages of e - safety.

A key component of E-Safety teaching will be around 'Sexting' (in KS2). This will focus upon:

---

There have been an increasing number of incidents where young people have shared sexual images of themselves (referred to as 'sexting'). Where this happens, images have usually been shared with a partner or intended partner as a form of flirtation or - in the eyes of the young person - 'safe sex'. Sometimes this is as a result of pressure, however.

Whatever had prompted the sending of the image, the act itself poses a risk to the young person in the image: once it has been shared it is liable to be distributed further. The young person is then exposed to risk of high-level bullying and to the possibility of being stalked by a paedophile who has become fixated on them after finding the image online.

Young people of an age likely to consider such actions should be educated about the risks.

Any incidents that come to light should be handled carefully, bearing in mind both that possession of the images may constitute an offence in itself, and the child or young person whose image has been shared is at risk and may already be subject to an exploitative relationship.

There have been a number of cases of images or video of children or young people under the age of 16 engaging in sexual activity being shared. These are legally images of child sexual abuse, even if they have been shared by others of the same age. All such cases are evidence of a child or young person being sexually exploited and should be dealt with as such.

If images or video of children engaged in sexual activity or in revealing poses are known to have been posted online, the following guidelines should be followed:

- The Police should be contacted immediately. The police will be in a position to make judgments about how matters are pursued in relation to offences and offenders. Where young people are voluntarily sending/sharing sexual images or content with one another the police may use the 'outcome 21' recording code to record that a crime has been committed but that it is not considered to be in the public interest to take criminal action against the people involved. This reduces stigma and distress for children and helps to minimise the long term impact of the situation. See **College of Policing, Briefing Note: Police Action in response to Youth Produced Sexual Imagery ('Sexting')**.;
- The nominated person for child protection/safeguarding should initiate an Early Help Assessment (EHA). Through the EHA process judgments will be made about the best means of supporting the child;
- Sites or networks on which the images appear should be alerted to the existence of illegal material. It is important that material online be removed as soon as possible, but staff must not put themselves at risk of illegality. Once the matter has been reported to the police their advice on this must be followed;
- Any young people who have themselves posted potentially illegal material should be told to remove the items, and warned that police action may follow if they do not. Through the EHA process, parents may also be involved;

- In some cases there may not be an obvious means of flagging or reporting the image. Even in these circumstances the existence of the image should be notified to the network provider and police action may be necessary to ensure its removal or engage the co-operation of the young person who has control of the image;
- The incident should be logged through the organisation's own monitoring / line management procedures;

**Appropriate educational/pastoral work should be undertaken with all young people involved.**

### **Sharing of nudes and semi-nudes ('sexting')**

This approach based on guidance from the UK Council for Internet Safety for all staff and for DSLs and senior leaders.

### **Your responsibilities when responding to an incident**

If you are made aware of an incident involving the consensual or non-consensual sharing of nude or semi-nude images/videos, including pseudo-images, which are computer-generated images that otherwise appear to be a photograph or video (also known as 'sexting' or 'youth produced sexual imagery'), you must report it to the DSL immediately.

You must **not**:

- › View, copy, print, share, store or save the imagery yourself, or ask a pupil to share or download it (if you have already viewed the imagery by accident, you must report this to the DSL)
- › Delete the imagery or ask the pupil to delete it
- › Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery (this is the DSL's responsibility)
- › Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- › Say or do anything to blame or shame any young people involved

You should explain that you need to report the incident and reassure the pupil(s) that they will receive support and help from the DSL.

### **Initial review meeting**

Following a report of an incident, the DSL will hold an initial review meeting with appropriate school staff – this may include the staff member who reported the incident and the safeguarding or leadership team that deals with safeguarding concerns. This meeting will consider the initial evidence and aim to determine:

- › Whether there is an immediate risk to pupil(s)

- › If a referral needs to be made to the police and/or children's social care
- › If it is necessary for the DSL only to view the image to safeguard the child or young person. That decision should be based on the professional judgement of the DSL. (*in most cases, images or videos should not be viewed*)
- › What further information is required to decide on the best response
- › Whether the image(s) has been shared widely and via what services and/or platforms (this may be unknown)
- › Whether immediate action should be taken to delete or remove images or videos from devices or online services
- › Any relevant facts about the pupils involved which would influence risk assessment
- › If there is a need to contact another school, college, setting or individual
- › Whether to contact parents or carers of the pupils involved (in most cases parents/carers should be involved)

The DSL will make an immediate referral to police and/or children's social care if:

- › The incident involves an adult. Where an adult poses as a child to groom or exploit a child or young person, the incident may first present as a child-on-child incident. See appendix 4 for more information on assessing adult-involved incidents
- › There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example, owing to SEND)
- › What the DSL knows about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- › The imagery involves sexual acts and any pupil in the images or videos is under 13
- › The DSL has reason to believe a pupil is at immediate risk of harm owing to the sharing of nudes and semi-nudes (for example, the young person is presenting as suicidal or self-harming)

If none of the above apply then the DSL, in consultation with the headteacher and other members of staff as appropriate, may decide to respond to the incident without involving the police or children's social care. The decision will be made, the reasons why the decision was made, and recorded in line with the procedures set out in this policy.

#### **Further review by the DSL**

If at the initial review stage a decision has been made not to refer to police and/or children's social care, the DSL will conduct a further review to establish the facts and assess the risks.

They will hold interviews with the pupils involved (if appropriate).

If at any point in the process there is a concern that a pupil has been harmed or is at risk of harm, a referral will be made to children's social care and/or the police immediately.

### **Informing parents/carers**

The DSL will inform parents/carers at an early stage and keep them involved in the process, unless there is a good reason to believe that involving them would put the pupil at risk of harm.

### **Referring to the police**

If it is necessary to refer an incident to the police, this will be done through, GMP, School Engagement Officer, local neighbourhood police, dialling 101, online report.

### **Recording incidents**

All incidents of sharing of nudes and semi-nudes, and the decisions made, the reasons why the decision/s was made in responding to them, will be recorded. The record-keeping arrangements set out in section 14 of this policy also apply to recording these incidents.

### **Curriculum coverage**

Pupils are taught about the issues surrounding the sharing of nudes and semi-nudes as part of our RSE/PHSE/ relationships and sex education and computing programmes. Teaching covers the following in relation to the sharing of nudes and semi-nudes:

- › What it is
- › How it is most likely to be encountered
- › The consequences of requesting, forwarding or providing such images, including when it is and is not abusive and when it may be deemed as online sexual harassment
- › Issues of legality
- › The risk of damage to people's feelings and reputation

Pupils also learn the strategies and skills needed to manage:

- › Specific requests or pressure to provide (or forward) such images
- › The receipt of such images

The policy on the sharing of nudes and semi-nudes is also shared with pupils so they are aware of the processes the school will follow in the event of an incident.

Teaching follows best practice in delivering safe and effective education, including:

- › Putting safeguarding first
- › Approaching from the perspective of the child
- › Promoting dialogue and understanding
- › Empowering and enabling children and young people
- › Never frightening or scare-mongering
- › Challenging victim-blaming attitudes

## **Education & Training – Staff**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

*A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process. All staff will receive training as part of the school's annual safeguarding sessions.*

### *Sessions*

*All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies*

Training sessions for parents will take place regularly.

### Education and Training – Parents and Governors





It is essential that Governors and parents receive e-safety awareness and/or training and understand their responsibilities. Training will be offered as follows:

*As part of Salford LEA's Governor Training provision.  
As an agenda item at Full Governing Body meetings.*

## **Communication devices and methods**

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

Communication method or device	Staff & other adults				Students/Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Mobile phones may be brought to school	†					†		
Use of mobile phones in lessons (at Headteacher's discretion)		†						†
Use of mobile phones in social time	†							†
Taking photos or videos on personal mobile phones or other camera devices (providing a clear educational purpose is evident)		†				†	†	
Use of personal hand held devices eg PDAs, PSPs	†							†
Use of personal email addresses in school, or on school network	†						†	
Use of school email for personal emails	†							†

Use of chat rooms / facilities		†					†	
Use of instant messaging		†					†	
Use of social networking sites		†						†
Use of blogs		†					†	





This table indicates when some of the methods or devices above may be allowed:

Communication method or device	Circumstances when these may be allowed	
	Staff & other adults	Students/Pupils
Mobile phones may be brought to school	N/A	Headteacher's permission Y6 to follow written stipulation (see attached)
Use of mobile phones in lessons	Clear education purpose i.e. <i>Tweeting / Blogging</i>	N/A
Use of mobile phones in social time	<i>during breaks or after school</i>	N/A
Taking photos on personal mobile phones or other camera devices	N/A	Headteacher's permission i.e. <i>residential trip</i>
Use of personal hand held devices eg PDAs, PSPs	N/A	N/A
Use of SMART Watches		<i>Not Allowed</i>
Use of personal email addresses in school, or on school network	<i>Clear educational purpose</i>	N/A
Use of school email for personal emails	<i>Clear educational purpose</i>	N/A
Use of chat rooms / facilities	<i>Clear educational purpose</i>	N/A

Use of instant messaging	<i>Clear educational purpose</i>	<i>N/A</i>
Use of social networking sites	<i>Clear educational purpose</i>	<i>N/A</i>
Use of blogs	<i>Clear educational purpose</i>	<i>N/A</i>
Use of 'Airtags' and similar	<i>N/A</i>	<i>Not Allowed</i>

### *Unsuitable/inappropriate activities*

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

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<b>User Actions</b>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
child sexual abuse images					<input checked="" type="checkbox"/>
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					<input checked="" type="checkbox"/>
adult material that potentially breaches the Obscene Publications Act in the UK					<input checked="" type="checkbox"/>
criminally racist material in UK					<input checked="" type="checkbox"/>
Pornography					<input checked="" type="checkbox"/>
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					<input checked="" type="checkbox"/>
promotion of racial or religious hatred					<input checked="" type="checkbox"/>

threatening behaviour, including promotion of physical violence or mental harm					✗
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✗	
Using school systems to run a private business				✗	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school				✗	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✗	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✗	
Creating or propagating computer viruses or other harmful files				✗	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✗	
On-line gaming (educational)		†			
On-line gaming (non educational)				†	
On-line gambling				†	
Accessing the internet for personal or social use (e.g. online shopping, banking etc)	†				
File sharing e.g. music, films etc				†	
Use of social networking sites	†				
Use of video broadcasting eg Youtube	†				
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)	†				



This table indicates when some of the methods or devices above may be allowed:

	<b>Circumstances when these may be allowed</b>
--	--

<b>User Actions</b>	<b>Staff &amp; other adults</b>	<b>Students/Pupils</b>
On-line gaming (educational)	<i>Clear educational purpose</i>	<i>Clear educational purpose</i>
On-line gaming (non educational)	N/A	N/A
On-line gambling	N/A	N/A
Accessing the internet for personal or social use (e.g. online shopping, banking etc)	<i>During break or social times</i>	<i>Clear educational purpose</i>
File sharing e.g. music, films etc	N/A	N/A
Use of social networking sites	<i>Clear educational purpose</i>	
Use of video broadcasting eg Youtube	<i>Clear educational purpose</i>	<i>Clear educational purpose</i>
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)	<i>Clear educational purpose</i>	<i>Clear educational purpose</i>

<b>Good Practice Guidelines</b>	
Email	
	<b>DO</b>
Best practice	Staff and students/pupils should only use their school email account to communicate with each other
Safe practice	Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping
Poor practice	<b>DO NOT</b>
	Staff: do not use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

<b>Good Practice Guidelines</b>	
Images, photos and videos	
	<b>DO</b>
Best practice	Only use school equipment for taking pictures and videos. Ensure parental permission is in place
Safe practice	Check the e-safety policy for any instances where using personal devices may be allowed.  Always make sure you have the Headteacher/SLT knowledge or permission  Make arrangements for pictures to be downloaded to the school network immediately after the event.  Delete images from the camera/device after downloading
Poor practice	<b>DO NOT</b>
	Do not download images from organisation equipment to your own equipment.  Do not use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

	Do not retain, copy or distribute images for your personal use.
--	---

<b>Good Practice Guidelines</b>	
Internet	
	<b>DO</b>
Best practice	Understand how to search safely online and how to report inappropriate content.
Safe practice	<p>Staff and students/pupils should be aware that monitoring software will log online activity.</p> <p>Be aware that keystroke-monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians.</p>
Poor practice	<b>DO NOT</b>
	<p>Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings</p> <p>Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.</p>

<b>Good Practice Guidelines</b>	
Mobile Phones	
	<b>DO</b>
Best practice	<p>Staff: If you need to use a mobile phone while on school business (trips etc), the school will should provide equipment for you.</p> <p>Make sure you know about inbuilt software/ facilities and switch off if appropriate.</p>
Safe practice	<p>Check the e-safety policy for any instances where using personal phones may be allowed.</p> <p>Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first</p>

Poor practice	<b>DO NOT</b>
	Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.
	Don't retain student/pupil/parental contact details for your personal use.

<b>Good Practice Guidelines</b>	
Social networking (e.g. Facebook/Twitter)	
	<b>DO</b>
Best practice	If you have a personal account, regularly check all settings and make sure your security settings are not open access.  Ask family and friends to not post tagged images of you on their open access profiles.
Safe practice	Do not accept people you do not know as friends.  Be aware that belonging to a 'group' can allow access to your profile.
Poor practice	<b>DO NOT</b>
	Do not have an open access profile that includes inappropriate personal information and images, photos or videos. Staff: Do not accept students/pupils or their parents as friends on your personal profile. Do not accept exstudents/pupils users as friends. Do not write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

<b>Good Practice Guidelines</b>	
Webcams	
	<b>DO</b>
Best practice	Make sure you know about inbuilt software/facilities and switch off when not in use.
Safe practice	Check the e-safety policy for any instances where using personal devices may be allowed.

	<p>Always make sure you have the Headteacher/SLT knowledge or permission</p> <p>Make arrangements for pictures to be downloaded to the school network immediately after the event.</p> <p>Delete images from the camera/device after downloading.</p>
<p>Poor practice</p>	<p><b>DO NOT</b></p>
	<p>Do not download images from organisation equipment to your own equipment.</p> <p>Do not use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.</p> <p>Do not retain, copy or distribute images for your personal use.</p>

## Incident Management

Incidents (students/pupils):	Refer to class teacher	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
<p>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)</p> <p>Unauthorised use of non-educational sites during lessons</p> <p>Unauthorised use of mobile phone/digital camera / other handheld device</p> <p>Unauthorised use of social networking/ instant messaging/personal email</p> <p>Unauthorised downloading or uploading of files</p> <p>Allowing others to access school network by sharing username and passwords</p> <p>Attempting to access or accessing the school network, using another student's/pupil's account</p> <p>Attempting to access or accessing the school network, using the account of a member of staff</p> <p>Corrupting or destroying the data of other users</p> <p>Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature</p> <p>Continued infringements of the above, following previous warnings or sanctions</p> <p>Actions which could bring the school into disrepute or breach the integrity of the ethos of the school</p>	Case by Case basis: See <i>Behaviour Policy</i>								

Using proxy sites or other means to subvert the school's filtering system	
Accidentally accessing offensive or pornographic material and failing to report the incident	

Deliberately accessing or trying to access offensive or pornography

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Incidents (staff and community users):	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	Case by Case basis, in line with Staff Acceptable Usage Policy & Code of Conduct						
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email							
Unauthorised downloading or uploading of files							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account							
Careless use of personal data eg holding or transferring data in an insecure manner							
Deliberate actions to breach data protection or network security rules							
Corrupting or destroying the data of other users or causing							

deliberate damage to hardware or software	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	
Actions which could compromise the staff member's professional standing	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	
Using proxy sites or other means to subvert the school's filtering system	
Accidentally accessing offensive or pornographic material and failing to report the incident	
Deliberately accessing or trying to access offensive or pornographic material	
Breaching copyright or licensing regulations	
Continued infringements of the above, following previous warnings or sanctions	

Further information and support

**For a glossary of terms used in this document:**

<http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf>

**For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:**

<http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf>

**R u cyber safe?**

**E-safety tips about how to stay safe online:** <http://www.salford.gov.uk/rucybersafe.htm>

## **Pupil Acceptable Use Agreement**

*These rules will keep me safe, keep my information private, and help me to be fair to others.*

I will only use the school's computers for schoolwork and homework.

I will not attempt to read any personal information on paper or in a computer file unless that information is meant for me.

I will only edit or delete my own files and not look at, or change, other people's files without their permission

I will keep my logins and passwords secret.

I will not attempt to learn logins and passwords that belong to other people. I will never use a school device whilst logged on as another pupil.

I will 'sign out' or 'log-off' after using any school device.

I will not bring files into school without permission or upload inappropriate material to my workspace.

I am aware that some websites and social networks have age restrictions and I will respect this.

I am aware that any website I visit / anything I type onto a device is monitored via our 'Securely' system which is monitored by our teachers.

I will not attempt to visit Internet sites that I know the school has banned.

I will only e-mail the people I know, or those a responsible adult has approved.

The messages I send, or information I upload, will always be polite and sensible.

I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

I will maintain my data and personal security: I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will *never* arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I understand that if I misuse any school device then I may be asked to not use it again for a given period.

I will immediately report any damage to any school device to my teacher.

I will not change the desktop background or screen saver on any school device.

I will only bring a mobile phone to school if I do the following:

- My parents have signed the agreement form
- I am walking home
- It is switched off and not used on the school premises at any time

*I have read and understand these rules and agree to sign for them on behalf of my child.*

*Parent Signature:* ..... *Date:* .....

*Child's name:* .....

31<sup>st</sup> March 2023

Dear Year 6 Parents and Carers,

We are writing to you in response to conversations held recently with several parents of our Year 6 pupils. Many parents have expressed a wish that, if their child either walks to or from school without adult supervision, then they would feel more at ease if a mobile phone could be carried by their child. The proposal has been discussed by our Senior Leadership Team and ratified by the Governing Body. As a result, we can clarify the following school rules around mobile phones which will come into place in the summer term after Easter:

- Only Y6 pupils who walk either to or from St. Philip's without adult supervision will be able to bring a mobile phone to school. This must be requested in advance from parents by completing the permission slip below.
- Mobile phones will be handed-in at 8:35 as the children enter the building. They will be kept in a named, sealed zip-lock bag within a box which will be stored away from the classroom in a secure place. The phones will be returned to pupils as they leave at home time.
- No mobile phone will be allowed to be used on any part of the school premises by children. They must remain switched off and in bags. This includes before 8:35 and after 15:10. **Any visible mobile phone will be taken to the school office and then only returned to a parent.**
- Mobile phones will not be taken with pupils to sporting events, trips or residential holidays away from school.
- An updated version of our E-Safety agreement will be signed by pupils to ensure they take understand are behave responsibility with a mobile phone.
- Parents who agree to allow their child to bring a mobile phone into school must sign the disclaimer below to accept that the school will not be liable for any damage or potential loss of equipment.
- It will be discouraged for pupils who attend after-school clubs or tuition to walk home independently as the local area is much quieter with fewer adults present at these times (see safety information below). Therefore, a mobile phone would not be necessary on these days.

We realise that the above mobile phone regulations are both comprehensive and stringent but, without these systems, it would not be possible for children to bring mobile phones into school. Please be aware that the local police recommend that primary school children do not carry mobile phones around school times as it makes them a potential target for robbery, bullying and it also significantly raises their risk of being involved in a road traffic accident. As a result, we are trying to offer parents the flexibility of allowing mobile phones to those who walk to or from school alone whilst ensuring we do all we can keep both children and staff safe. We will be ensuring that we work with our children to promote and encourage the safe

use of a mobile phone when walking to and from school. We ask that parents and carers also discuss the importance of this at home too.

If you wish for your child to walk to / from school without adult supervision, for them to carry and mobile phone and you are happy to support the school's mobile phone safety systems then please complete the form below and return to your child's class teacher:

-----  
-----

Child's Name: \_\_\_\_\_ Class Teacher: \_\_\_\_\_

I accept that St. Philip's RC cannot accept responsibility for any damage to or loss of a child's mobile phone

I am happy to support the school's mobile phone safety systems listed above

Parent Name: \_\_\_\_\_ Parent Signature: \_\_\_\_\_

My child will be walking without adult supervision on:

Monday before school	<input type="checkbox"/>	Monday after school	<input type="checkbox"/>
Tuesday before school	<input type="checkbox"/>	Tuesday after school	<input type="checkbox"/>
Wednesday before school	<input type="checkbox"/>	Wednesday after school	<input type="checkbox"/>
Thursday before school	<input type="checkbox"/>	Thursday after school	<input type="checkbox"/>
Friday before school	<input type="checkbox"/>	Friday after school	<input type="checkbox"/>

If you have any questions or suggestions regarding the mobile phone safety system then please contact me via the school office,

Miss R McNamara	Headteacher
Mr. J. Cooper	Assistant Headteacher
Miss C. Lavelle	Assistant Headteacher

## **Staff, Volunteer and Community User Acceptable Use Policy**

St. Philip's RC Primary School

### **General Data Protection Regulation**

### **Acceptable Use Policy 2018**

#### **Introduction**

St Philip's RC Primary School commits to protecting the privacy and security of the personal information it holds for staff, governors and volunteers. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This agreement covers all digital and physical data systems, e.g. the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.

I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.

School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. Such misuse is also covered by the GDPR, and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT stems and other users. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate. I will not use personal equipment to access school data.

I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.

I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the school network to upload any work documents and files in a password-protected environment. I will protect the devices in my care from unapproved access or theft (including the encryption of all devices including external memory). I will not share any files or folders on the school network with any other user. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from site. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.

I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

I will respect copyright and intellectual property rights.

I have read and understood the school's Data Security Policy and e-Safety Policy which cover the security of data and safe and appropriate access to data.

I will report all incidents of concern regarding children's online safety to the Designated Child Safeguarding Lead/Lead for Prevent (Ruth McNamara, Headteacher). I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-Safety Coordinator.

I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.

My communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will ensure that a BCC of any emails to parents/carers are sent to: [ruth.mcnamara@salford.gov.uk](mailto:ruth.mcnamara@salford.gov.uk). All written notes will be copied to the school Office Manager. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.

My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of

communication will not interfere with my work duties and will be in accordance with the school AUP and the Law.

Any such communication will be professional in tone and manner. This includes my usage of social media (on any device). I will not be 'friends' with or 'follow' or 'interact' with any parent of a pupil/former pupil within the school, including those who are still within the education system.

I will set all of my social media accounts to 'private' settings and will support of the e-safety officer if unsure of how to do this.

I will not create, transmit, display, write, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

I will promote e-Safety (including privacy) with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create. Similarly, I will promote care for others in the pupils' writing and any other content that they create.

I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The school may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I \_\_\_\_\_ (please print name) acknowledge that I have received and read and understood a copy of the St. Philip's RC Primary School's Acceptable Use Policy.

Signed \_\_\_\_\_

Dated \_\_\_\_\_

STAFF TAPESTRY DECLARATION.

As a member of staff at St Philip's R.C. School, you will be expected to use Tapestry to observe children within the setting. All staff must agree and sign the following declaration:

- I agree to use photographs/ videos containing images of all children for professional use only.
- I will not take photos or videos of any child on any device other than those supplied by the school.
- I will not remove or copy photos or videos from Tapestry under any circumstance.
- I have read, understood and signed the school's 'Acceptable Use' Policy and agree to adhere to the terms in place.
- I will log out of the Tapestry app or program when I'm finished in order to maintain confidentiality.
- I will not share log in or password details with any person.
- I will take all responsible steps to ensure the safe keeping of any portable device e.g. iPad/tablet that I am using and report any missing devices immediately.
- I know how to contact Tapestry team at FSF HQ ([tapestry.support@eyfs.info](mailto:tapestry.support@eyfs.info)) so that we can temporarily deactivate your account / help you change passwords if your device is stolen and you suspect someone might be able to access your account.
- I will not set my browser to remember my Tapestry password.
- If accessing Tapestry at home, I will maintain confidentiality and professionalism.

Name of staff.....

Signed..... Date.....

STAFF TAPESTRY USAGE

As members of teaching staff at St Philip's R.C. School, we have agreed on the following to guide our usage of Tapestry:

- One individual and one group observation per child, per fortnight.
- For a child's voice in group observations, use the child's initials to show who said what.
- Observations to be uploaded to the journals every other Friday for parents to view.
- A lot of observations will be incidental, however a 'focused observation' should be planned in every two weeks. This should be reflective of any gaps in curriculum and linked to planning.
- Care will be taken with SPAG, adding FLAGS and TAGGING THE RIGHT CHILD. This should be double checked when we upload to the journals every other Friday.
- Teachers need to oversee observations made by TA's and add the relevant FLAGS. Please also check for SPAG and that the observation is relevant.
- During normal school operation, parents will only be able to add their own observations and edit them. Teachers should acknowledge these observations by 'liking them'.
- To help get parents and staff familiar with Tapestry, homework challenges could be set as part of the usual homework e.g. Can you take a picture of the things you found on your sound hunt and record this on Tapestry?

Name of staff.....

Signed..... Date.....

## **Appendix 3: 'Airtag' Policy**

### **Purpose of This Guidance**

The purpose of this guidance is to outline the school's position on the use of tracking tags such as Apple AirTags on children. While we understand that parents may have concerns about their child's safety, the use of such devices raises significant safeguarding, privacy, and security concerns. As such, the use of tracking tags on school trips is not permitted.

### **Key Concerns**

#### **1. Privacy and Data Protection**

o Tracking devices can raise significant privacy concerns as they can track a child's location without their informed consent.

o Schools have a duty to protect all children's personal data, and the use of tracking devices could compromise this responsibility.

#### **2. Safeguarding Risks**

o Tracking devices can inadvertently reveal the real-time location of a group of children, which poses a significant risk—especially for pupils under protection orders, in foster care, or with specific safeguarding needs.

o If lost or misplaced, a tracking device could be misused, potentially putting a child at risk.

o Parents using tracking devices to post the exact location of a class or group of children on social media platforms, places the safety of all the children and staff at risk and specific children who may be fleeing Domestic Violence or who may be subject to court orders.

#### **3. Disruption to Pupil Management**

o Teachers and staff are responsible for the supervision and safety of all pupils during the school day. The use of tracking devices may create unnecessary confusion and interfere with established safety protocols.

#### **4. Other Implications**

- If a pupil is carrying a tracking device, teachers or other pupils might receive alerts, creating confusion or concern.
- If a tracking device beeps unexpectedly, it could cause unnecessary panic during a school trip.
- There's a risk of unauthorised individuals detecting or following a tracking device, making it a potential security and safeguarding issue.

### **School Policy on Tracking Devices**

- In line with this school guidance, personal tracking devices such as AirTags are not permitted on the school premises for usage by children.
- Parents should trust the school's supervision and safeguarding policies, which are designed to ensure children's safety at all times.
- If parents have specific concerns about their child's wellbeing during the school day, they should communicate these directly with the class teacher.
- Any tracking device found in use on a school trip will be removed and returned to parents at the end of the school day.

### **Alternative Safety Measures**

- Schools will continue to implement rigorous safeguarding procedures, including appropriate staff to pupil ratio, regular headcounts, buddy systems, and designated meeting points.
- Staff will always be available to support and supervise pupils throughout the trip.
- Parents will be provided with clear contact information should they need to reach the school during the trip.

By implementing this policy, we aim to maintain a safe, secure, and well-organised environment for all children during the school day. We appreciate the cooperation of parents and guardians in ensuring that all pupils remain safe whilst educated at St. Philip's.

# St Philip's RC Primary School

## General Data Protection Regulation GDPR

### Privacy Notice for Staff

#### Introduction

Staff employed by St Philip's RC Primary School ] and contractors engaged by the school have many legal rights regarding how their personal data is obtained, stored, processed and transmitted (i.e. 'processed') both during your period of employment and after. The school has to obtain certain information before a contract of employment may be offered. This privacy notice details how the school will comply with the law and gives you an understanding of why and how the school uses the information about you.

This privacy notice does not form part of your contract of employment. The notice may be updated at any time. All people working with or for the school must comply with this policy when processing data.

The Governing Body and Leadership of St Philip's RC Primary School acknowledge the absolute necessity for correct and lawful treatment of data and are committed to ensuring security for your data.

#### Roles and Responsibilities

The school is a **Data Controller** as we are responsible for decisions about how and why we use your personal information.

At times the school acts as a **Data Processor** when we are required to obtain, process and transfer data on the behalf of external organisations.

The school has appointed a **Data Protection Officer**

Ben Cain

Tel: 01924 907319

Address: First Floor, Unit A, Cedar Court Office Park, Denby Dale Road, Wakefield

Email: [dpo@feps.co.uk](mailto:dpo@feps.co.uk)

Usually, the school will coordinate data protection practice through Miss R MCNamara (Headteacher)

Ben Cain may be contracted directly should any employee or contractor feel that their concerns about data protection are not being addressed within the school. Among the DPO's duties are:

Advice on the secure storage and transmission of data (both physical and digital)

Updates for the school on the GDPR

The completion of a data audit

Support for a data processing record system

The provision of template GDPR documentation (please note that this cannot be shared beyond the school without the permission of Safeguarding Monitor)

Reporting to the school's leadership and governing body on levels of security and compliance

Support with securing certification that they are also complying fully with GDPR duties from third parties who might hold personal data through the school.

The DPO will communicate with the Information Commissioner's Office should there be a confirmed or suspected data breach.

The DPO will communicate with any person whose data might have been improperly accessed, deleted, lost or stolen.

The governor who oversees data security for the governing body is Mr Peter Riley, 01617924595.

### **The principles under which the school will process data**

Data will be kept securely - all employees and contractors share this duty.

Personal information will all be stored no longer than is necessary to exercise the school's duties and statutory requirements.

All employees and contractors will be informed clearly about the purposes for processing data.

Data processing will be limited to the purposes that are explained to employees and contractors.

The school will keep data relevant, current and up-to-date.

The school will only use personal information in a legal and transparent manner.

### **The categories of information and the bases for which that information is processed.**

In broad terms the school will collect, store, process and transmit data to meet its duties under

Employment law

Safer recruitment

Staff welfare

Payroll and pension procedures

Performance Management

To meet the school's responsibilities under the Equalities Act

### **Specifically the school will process the following information**

Data processed on the legal basis of public task for safe recruitment, promotion and pupil safeguarding

*Your application with references, proof of qualification, proof of identity, right to work in the UK, DBS certification, any disability, notes on your recruitment process, images captured within the school site by CCTV equipment, your use of IT equipment to ensure compliance with our Acceptable Use Policy and other IT policies*

Data processed on the legal basis of public task for employment, payroll and pension procedures and the prevention of fraud

*Your data of birth, bank details, payroll details, address, pension choices, national insurance number, a photograph of you, tax status, car details (if you intend to park in the school site), leave entitlement, sick leave monitoring and any disciplinary or capability notes should the need arise*

Data processed on the legal basis of public task for staff welfare

*Contact details for your next of kin, any medical needs, disability, allergies and any other health needs that you choose to share*

Data processed on the legal basis of public task to fulfil the school's duty of accountability

*Your performance management, the attainment and achievement of pupils you teach or for whom you share a responsibility, your continuous professional development*

Data processed on the legal basis of consent for equality monitoring

*You may choose to disclose information regarding your ethnicity, age, religion, gender, sexual orientation and medical needs so that the school can monitor its equality of employment*

Data processed on the legal basis of consent to support the school team's social life

*With your consent the school use your data to share information about social events organised for the staff*

Data processed on the legal basis of consent to support the school's professional relationships

*Your trade union membership*

This cannot be an exhaustive list, but any further information will be collected and used legally and on either the basis of public task or consent. Much of the information is collected during recruitment and induction. We have to collect some information from former employees and other agencies such as the **Data Barring Service**. Further information will be collected throughout your period of working for the school. Some information will be processed for external agencies, including future employers on the basis of public task. The principal use of your information will be for the school to perform the contract that applies to our working relationship.

If information required on the basis of the school's public task is withheld then the school might not be able to perform the contract that applies to our working relationship.

You will be notified if we need to use your information in ways other than those so far stated and you will be informed about which legal basis has been selected.

The school regards certain information as particularly sensitive - such as information on physical and mental health, religion, ethnicity and sexuality. Such information will be gathered to support the school's equal opportunities obligations, but will only be gathered given your specific written consent. Such information may also be used to ascertain your fitness to work and to ensure your health and safety and/or to make reasonable adjustments to your working environment and work pattern.

The school does not use your information for automated decision making.

We share some information with third parties most commonly for HR tasks and as required by the law

*Payroll and pension, benefits provision and administration*

All third parties are required to maintain data security as the law requires.

We require certification from third parties that your information is secure.

After your period of employment with the school we will only keep that information which we are required to do so to fulfil financial, legal and safeguarding duties.

### **Your duty to inform the school of changes**

The school must have up-to-date information which is accurate. Please keep the school informed of any changes to your information while you are employed by the school

### **Your rights to 'see' your data**

Under law, under most circumstances, you have the right to request access to your personal information (usually this is known as a 'data subject request'). Under this right you may request a copy of the information we hold on you and to check that processing is lawful.

You may request correction or completion of any of the data.

You may request that your personal information is erased or restricted if there is information for which there is no good purpose for the school to continue to hold

Please contact Miss R McNamara [**school GDPR Lead**] in writing should you wish to review, correct or erase personal information, or you may contact the DPO directly. The school has 15 days to meet your request.

Please note that the school has a primary duty of care to the children and may withhold access if it can be demonstrated that this is necessary in the vital interests of a child. You will be informed if this is the case in writing.

There is no fee required for your access to data or for any amendments.

You have the right to withdraw the consent that you have previously granted the school to process certain data. If this is the case then please contact Miss R McNamara [**school GDPR Lead**] in writing.

### **School compliance**

St Philip's RC Primary School has appointed a Data Protection Officer to oversee compliance with this privacy notice. If you have any questions about your data security or this privacy notice, then please contact the DPO initially.

You have the right to make a complaint to the Information Commissioner's Office (ICO) which is the UK supervisory authority for data protection.

St Philip's RC Primary School may update this privacy notice at any time. A copy of the new notice will be given to you. We may inform you in other ways of any changes that we make to the processing of your data.

I \_\_\_\_\_ (please print name) acknowledge that I have received and read and understood a copy of St Philip's RC Primary School **privacy** notice.

Signed \_\_\_\_\_

Dated \_\_\_\_\_

## **Appendix 2.2 – Governors Privacy Notice**

### **St Philip’s RC Primary School**

### **General Data Protection Regulation**

### **Privacy Notice for Governors**

#### **Introduction**

Governors supporting St Philip’s RC Primary School have many legal rights about how their personal data is obtained, stored, processed and transmitted (i.e. ‘processed’) both during your period on the governing board and after. The school has to obtain certain information before a candidate for the governing body may stand for election; further information has to be passed on to the DfE, the LA and diocese. This privacy notice details how the school will comply with the law and gives you an understanding of why and how the school uses the information about you. This privacy notice is not a form of contract.

The Governing Body and Leadership of St Philip’s RC Primary School acknowledge the absolute necessity for correct and lawful treatment of data and are committed to ensuring security for individual governor’s data.

#### **Roles and Responsibilities**

The school is a **Data Controller** as we are responsible for decisions about how and why we use your personal information (for example collecting contact information to organise meetings effectively).

At times the school acts as a **Data Processor** when we are required to obtain, process and transfer data on the behalf of external organisations (certain details about governors have to be passed on to the DfE, for example).

The school has appointed a **Data Protection Officer**

Claire Lockyr  
Impero Software  
Oak House,  
Mere Way,  
Ruddington Fields Business Park,  
Nottingham, NG11 6JS, UK  
+44 (0) 330 4004142

The school will coordinate data protection practice through Miss R McNamara, Headteacher.

Claire Lockyr may be contracted directly should any governor feel that their concerns about data protection are not being addressed within the school or the rest of the governing body. Amongst the DPO’s duties are:

Advise the secure storage and transmission of data (both physical and digital)

Updates for the school on the GDPR

The completion of a data audit

Support for a data processing record system

The provision of template GDPR documentation (please note that this cannot be shared beyond the school without the permission of Safeguarding Monitor)

Reporting to the school's leadership and governing body on levels of security and compliance

Support with securing from third parties who might hold personal data through the school certification that they are also complying fully with GDPR duties

The DPO will communicate with the Information Commissioner's Office should there be a confirmed or suspected data breach

The DPO will communicate with any person whose data might have been improperly accessed, lost or stolen

The governor who oversees data security for the governing body is Mr Peter Riley 01617924595.

### **The principles under which the school will process data**

Data will be kept securely - all governors share this duty

Personal information will all be stored no longer than is necessary to exercise the school's duties and statutory requirements

All governors will be informed clearly about the purposes for processing data

Data processing will be limited to the purposes that are explained to governors

The school will keep data relevant, current and up-to-date

The school will only use personal information in a legal and transparent manner

### **The categories of information and the bases for which that information is processed**

In broad terms the school will collect, store, process and transmit data to meet its duties under

Safer recruitment (which governors have the relevant training)

Governor welfare (should it be thought wise to keep next-of-kin details)

Attendance details (meetings)

To meet the school's responsibilities under the Equalities Act and to meet the national guidance on the recruitment of governors

Specifically the school will process the following information

*Data processed on the legal basis of public task for safe recruitment - which governors may lead recruitment following successful training in safer recruitment*

Data processed on the legal basis of public task

*Your fitness to acquire the role of school governor (the declaration governors sign when standing for office). The category within which you will serve as a governor (such as a parent governor). The names of nominees.*

Data processed on the legal basis of public task for governor welfare

*Contact details for your next of kin, any medical needs, disability, allergies and any other health needs that you choose to share*

Data processed on the legal basis of public task to fulfil the school's duty of accountability

*The roles that you agree to take on within the board of governors. The numbers of meetings attended and the training that you acquire in your role as governor.*

Data processed on the legal basis of consent for equality monitoring

*The DfE requires data on the background of governors to be registered by the Headteacher or their representative. This data may include ethnicity, country of birth and gender*

*This cannot be an exhaustive list, but the school will inform members of the governing body of any significant extra data processing that involved governors' personal information.*

*Following DfE advice this school requires that all governors have their background checked with the Disclosure and Barring Service as they have a role of responsibility for vulnerable children.*

*If significant information is withheld then a candidate for the role of governor might not be able to stand for election.*

Certain categories of personal information are seen as particularly sensitive:

Data concerning health, including mental health

Data concerning children

Data relating to religion

Data relating to sexuality

Data relating to ethnicity

Data relating to performance management

Should the school process any governor's data from the above categories, then particular care will be taken and the data will be kept securely. Likewise the governors share a duty of care with such data and must treat data within these categories with enhanced confidentiality.

The school does not use automated decision making processes based on governors' data.

The school does require all third parties who have access to or also process school data, to confirm that they also meet the standards expected by the GDPR.

Under law, under almost all circumstances, you have the right to request access to your personal information that the school holds. Usually this is called a 'subject access request.' Under this right you may request a copy of the information that the school holds, to check the data and to check that the processing is lawful. Please note that 'subject access requests' cannot attract a fee, but that they do necessitate significant time and human resources. Should the school consider that responding to all aspects of a subject access request may be against the welfare interests of a child, then parts of an SAR may be withheld. In the very rare instance that this is the case, you would be informed in writing.

Should the school wish to hold data in addition to that which is required to maintain the welfare of the pupils, staff and the efficient management of the governing body, then this additional data may be processed on the legal basis of consent. Your consent would be sought, thereafter you would have the right to withdraw consent.

As well as seeking advice and taking complaints to the school's Data Protection Officer (see contact details above) individual governors may make a complaint to the Information Commissioner's Office (ICO) which is the UK supervisory authority for data protection.

It is likely that the EU GDPR will, with minimal alteration, become the Data Protection act 2018. Should this not be the case, the school will notify all schools users of significant changes to data protection law.

St Philip's RC Primary School may update this privacy notice at any time. A copy of the new notice will be given to you. We may inform you in other ways of any changes the we may make to the processing of your data.

I \_\_\_\_\_ (please print your name) acknowledge that I have read and received a copy of St Philip's RC Primary School governors' privacy notice.

Signed \_\_\_\_\_

Dated \_\_\_\_\_

Appendix 3 – Use of Images Consent Form



St. Philip's  
RC Primary School

## General Data Protection Regulation GDPR

### Request for consent

Dear Parents

Following the requirements of the General Data Protection Regulation we are writing to families about the use of photographs and videos which might record images of your child.

The school wishes to use photographs for the reasons listed below, but we need your consent (agreement) for this. We are particularly keen that we gain consent for the first purpose listed as we use photographs carefully to support the school's health and safety procedures. This helps us to ensure the best possible standards of pupil welfare.

Your consent will last as long as your child is a pupil at this school, or until you inform us that you want to change your consent.

We will write to you before your child leaves the school should we want to keep or continue to use any photographs of your child after your child leaves the school.

Please can we remind parents that they should follow any guidance at school events about taking photographs or videos? We all need to work together to respect each other's privacy wishes.

*I consent to the school using a photograph of my child \_\_\_\_\_ to support the school pupil welfare procedures.*

Yes

No

*I consent to the school using photographs and videos of my child to celebrate achievements in their classroom*

Yes

No

*I consent to the school using photographs and videos of my child to celebrate achievements in the school*

Yes

No

*I consent to the school using a photograph of my child to celebrate achievements beyond the school and in the press*

Yes

No

*I consent to the school using a photograph of my child to celebrate achievements beyond the school and online, and on the school's website and twitter page*

Yes

No

Signed \_\_\_\_\_

Dated \_\_\_\_\_

Please return this form to school office.

Appendix 4: Letter to Parents

## **General Data Protection Regulation GDPR**

Dear Parents

On May 25th a new Regulation comes into force, the General Data Protection Regulation.

The aim of the Regulation is to make personal information even more confidential than it already is, under the current Data Protection act. The Regulation affects all countries in the European Union, but it will remain in British Law following Brexit.

In the United Kingdom the Information Commissioner's Office will check that everyone is complying with the law.

The school has worked hard to ensure that we comply with the requirements of the Regulation, because we take your privacy seriously. We will include aspects of the GDPR in the IT and computing curriculum so that your children learn how to protect their privacy and online reputation in our highly technological world.

The school staff will soon have training so that they are familiar with the requirements of the GDPR. Our documentation is ready so you will soon see the school issuing fresh privacy notices and acceptable use policies for families and pupils. Families will also see new letters requesting consent for some school activities, such as for the use of photographs. Please note that we have to have a reply to these letters, otherwise your child might miss out when you would actually prefer them to be included: we cannot just assume that you agree or disagree.

We have reviewed the security of all our IT systems and the storage of our paper records. If any companies or partner agencies have access to any school data then we are requiring them to confirm that they also comply with the GDPR.

After May and our data audit we will start using a new system to record school's use of data. We will also be assessing how we collect and protect the most sensitive data to ensure security levels are as high as can be reasonably expected.

Thank you for your continued support as we all work to protect everyone's right to privacy.

Yours sincerely

Miss R McNamara

Headteacher



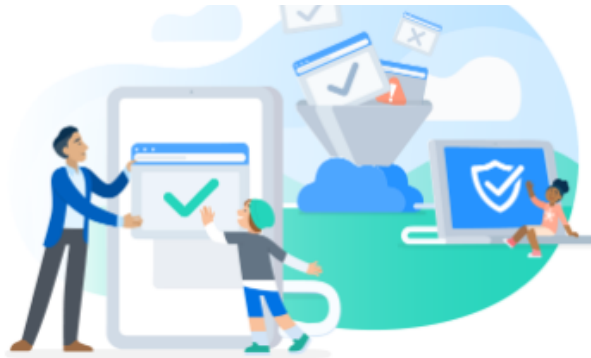
# Deliver safer online experiences

Ensure student safety on all devices, anywhere they go

[Request a trial](#)



Compatible with Apple, Microsoft, and Google devices



## Keep students safe with web filtering that puts you in control

Filter, a cloud-based web filter designed specifically for schools, helps you keep students safe with powerful features that make your school safer and your IT team happier. Get visibility into online activity, download or email reports, and block inappropriate sites instantly.



*Filter gives us peace of mind, especially when students have devices at home. Not only are we following our legal responsibilities and protecting students, but we are also opening up access and educational opportunities.*

**Michael Nikson**

Instructional Technology Coordinator, School District of

## Key advantages of Filter



### Cloud-based web filtering

Stay up-to-date with no bulky hardware, software crashes, agents, or network bottlenecks.



### Filters all devices

Chromebooks, iPads, Macs and PCs. Filter safeguards students across any device or operating system.



### Seamless authentication

Google, Azure, and Active Directory authentication using G Suite or Office 365.



### Easy setup

Go up and running in minutes, no hardware required.



### Scalable

School web filtering that delivers unlimited amounts of bandwidth and concurrent connections.



### Unlimited data retention

90 days of searchable data history.

## Simplify your workflow

Get easy-to-use and powerful tools designed especially for schools and busy IT teams.

- Cloud-based and scalable
- Live activity feed
- Instant site categorization  
Be confident that Innocent eyes are protected with geScan technology that automatically scans and categorizes new sites in a matter of seconds.
- Fast and helpful support



Click to enlarge image

## Customize to your heart's content

Go beyond CIPA compliance with web filtering that does everything you expect, with none of the hassle.











- YouTube controls
- Time-based policies  
Apply filtering rules based on schedules to accommodate after-school programs and clubs.

Click to enlarge image

## Filter every device, everywhere

Filter all of your school's traffic, all of the time — whether devices are on-campus, off-campus, or BYOD.

-  **Parent access**   
Give parents/caregivers control over and visibility into online activities when devices go home.
-  **Patented SmartPAC technology** 
-  **Selective SSL decryption** 
-  **Home and guest policies** 



Click to enlarge image

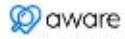
## See Filter in action

Make student safety simple with cloud-based web filtering designed specifically for schools.

[Get the brief](#)

[Try for 30 days](#)





## Know which students need help now

Intervene quickly to safeguard students against self-harm, suicide, bullying, and violence

[Get the brief](#)



## Identify at-risk students with student wellness monitoring

Aware gives you the ability to know which students are struggling so you can intervene quickly and early — before things get worse.



- Wellness levels**  
Use evidence-based wellness levels to identify students in need and allocate limited student services resources more effectively.
- Preventative tools**  
Address threats of bullying, violence, self-harm, and suicide early and effectively with powerful and proactive AI-enabled capabilities.
- Case management**  
Easily track cases from creation to resolution and maintain accurate case records by adding Respond.
- Real-time notifications**  
Know immediately if a student's activity indicates signs of nudity, bullying, suicide, or violence.
- Cross platform**  
Covers all your devices—including Chromebooks, iPads, Mac, and Windows, and on Google Drive and Microsoft Office 365 as well.
- Comprehensive analysis**  
Analyze all student activity across email, documents, social media, and web browsing using K-12 education's longest-learning AI.

## Gain visibility into students' mental health

Identify students who may be at risk so you can intervene where you're needed most.

- At-Risk AI
- Wellness levels**  
Rely on evidence-based wellness level monitoring to understand and visualize each student's current emotional state — and respond quickly if their level declines.
- Flagged activity alerts



[Click to enlarge image](#)

## Monitor for nudity, bullying, suicide, and violence

Know immediately about concerning student activities with unrivaled AI-powered analysis.

- Don't come 2 school tomorrow or you're going to get it...
- I would be better off dead. It's all too much can I just get it over with...
- I'm sorry for cutting, there's only so much I can take...

- Aware AI
- Nudity quarantine and recall
- Bullying detection and prevention

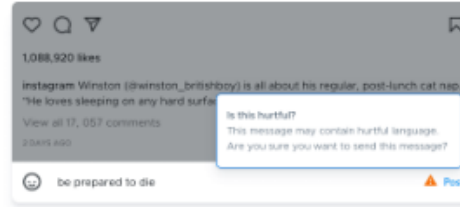
## Support students with preventative and automated interventions

Use proactive and preemptive tools to get in front of concerning student behaviors.

Helpful resources, right now

**Think twice before hitting send**

Address bullying before it happens with Think Twice's real-time prompts that encourage students to reconsider sending or posting messages that contain harmful language.



Click to enlarge image

## Streamline alert and case management

Centralize and streamline case management, and get 24/7 support from trained experts.



Click to enlarge image

Delegated alerts

Customizable notifications

Proven case management

**24/7 response**

Pair Aware with Securly On-Call to gain a team of highly-trained specialists, who analyze alerts round-the-clock and notify you of critical situations.

## See the students who need help with Aware

With Securly Aware, you know how your students are doing so you can focus your resources on the students who need support the most.

Don't worry about your students' wellness. Know for sure with Aware.

Get the brief

Request a demo

