St John and St Nicolas Schools Federation | For the good of all through curiosity, creativity and love

Policy Title:	**E-Safety Policy**
Policy Reference:	**SJN0076**
Description:	Procedures to safeguard all members of the federation community
Status:	Approved by Governing Board
Category:	Non-statutory *(based on model policy)*
Review frequency:	Every two years
Contact:	governors@stjohnandstnicolasschools.org.uk
Version:	**V1.1**
Other relevant policies:	Child protection, behaviour, complaints, safeguarding
Date for Review:	July 2027

Change Record				
Version Number	**Date Approved**	**Governing Board Minute Reference**	**Description of Amendments**	**Review Date**
1.0	*17.07.23*	*FGB Minutes 17.07.23*	*New policy recommended by policies working party and ratified by FGB*	*July 2025*
1.1	*21.10.25*	*FGB Minutes 21.10.25*	*Update version number, dates, format, contents page numbers*	*July 2027*
1.2				
1.3				
1.4				

Index		Page
1.	Introduction and overview	3
	• Rationale and scope	3
	• Roles & responsibilities	4
	• How the policy will be communicated to staff/pupils/community	7
	• Handling complaints	8
	• Review and monitoring	8
2.	Education and curriculum	8
	• Pupil e-safety curriculum	8
	• Staff and governor training	9
	• Parent awareness and training	9
3.	Expected conduct and incident management	9
	• Expected conduct	9
	• Incident management	9
4.	Managing the information and communications technology infrastructure	10
	• Internet access, security (virus protection) and filtering	10
	• Network management (user access, backup, curriculum and admin	10
	• Photographs and video of children	10
5.	Data security: management information system access and data transfer	11
	• Strategic operational practices	11
	• Technical solutions	11
6.	Equipment and digital content	11
	• Personal mobile phones and devices	11
	• Digital images and video	12
	• Asset disposal	12
	Appendices	
1.	Parental consent form (St John's)	13
2.	Parental consent form (St Nic's)	16

St John and St Nicolas Schools Federation
E-Safety Policy

At St John and St Nicolas Schools Federation, our vision is 'For the good of all – through curiosity, creativity and love.' This vision inspires everything that the federation does.
It applies equally to all the federation's policies with the intention that our policies impact as fairly and positively as possible to meet the needs of all members of our schools' community.

1: Introduction and overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St John and St Nicolas Schools Federation with respect to the use of the internet and all forms of communication technology
- Safeguard and protect the children, staff and governors of St John and St Nicolas Schools Federation
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyberbullying which are cross-referenced with other federation policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students

The main areas of risk for our federation community can be summarised as follows:

Content

- Exposure to, and sharing of, inappropriate content, including online pornography
- Ignoring age ratings in games (with e.g., violence associated with often racist language); substance abuse etc.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites, incitement to extremism
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation

- Health and well-being (amount of time spent online (internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as self-generated indecent images (SGII)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope
This policy applies to all members of the St John and St Nicolas Schools Federation community (including staff, pupils, governors, volunteers, parents, carers, visitors, community users) who have access to and are users of school information and communications technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The federation will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & key responsibilities
Everyone is expected to follow the e-safety policy

Executive headteacher
- To take overall responsibility for e-safety provision
- To take overall responsibility for data and data security
- To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- To be aware of procedures to be followed in the event of a serious e-safety incident.
- To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g., network manager)
- To communicate regularly with the senior leadership team and the governing board to discuss current issues, review incident logs and filtering / change control logs

Head of school
- To ensure that an e-safety incident log is kept up to date
- To liaise with the local authority and relevant agencies
- To take day to day responsibility for e-safety issues

Computing subject leader

- To take a leading role in reviewing the school e-safety policies / documents
- To promote an awareness and commitment to e-safeguarding throughout the school community
- To ensure that e-safety education is embedded across the curriculum
- To liaise with school information and communications technology (ICT) technical staff
- To facilitate training and advice for all staff
- To keep up to date with e-safety issues and legislation, 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 and use of social media
- To oversees the delivery of the e-safety element of the computing curriculum

Governors

- To ensure that the federation follows all current e-safety advice to keep the children and staff safe
- To approve the e-safety policy and review the effectiveness of the policy. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. The named governor for safeguarding is also the named e-safety governor
- To support the school in encouraging parents and the wider community to become aware of and engaged with e-safety activities

Computer support provider

- To report any e-safety related issues that arises, to the headteacher/designated person
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy
- To ensure that provision exists for misuse detection and malicious attack e.g., keeping virus protection up to date
- To ensure the security of the school information and communications technology (ICT) system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices:
    - The school's policy on web filtering is applied and updated on a regular basis
    - The local authority / web filtering provider is informed of issues relating to the filtering applied
    - That they keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
    - That the use of the network, remote access, data systems and email is regularly monitored in order that any misuse or attempted misuse can be reported to the headteacher for investigation, action or sanction

- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To keep up-to-date documentation of the federation's e-security and technical procedures

Data manager

- To ensure that all pupil data held on the school office machines is protected and has appropriate access controls in place

Teachers

- To embed e-safety issues in all aspects of the curriculum and other school activities
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws and creative commons licences

All staff

- To read, understand and help promote the federation's e-safety policy and guidance
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and to monitor their use - implementing current federation policies with regard to these devices
- To report any suspected misuse or problem to the executive headteacher or head of school
- To maintain an awareness of current e-safety issues and guidance e.g., through continuing professional development
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones etc.

Pupils

- To understand that children under the age of 13 are not permitted to be registered to use social media, including for example Facebook and Instagram. Therefore, no pupil in the federation should have a social media account
- To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To know and understand federation policy on the use of mobile phones, digital cameras and hand-held devices
- To know and understand federation policy on the taking / use of images and on cyber-bullying

- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To help the federation in the creation/ review of e-safety policies

Parents/carers

- To support the schools in promoting e-safety which includes the pupils' use of the Internet and the school's use of photographic and video images
- To ensure that all photographs and videos are for personal use only and are not to be shared on social media platforms
- To read, understand and promote the e-safety policy with their children
- To access the federation website in accordance with the e-safety policy
- To consult with their child's school if they have any concerns about their children's use of technology

External groups

- Any external individual / organisation will be expected to follow the e-safety policy

Communication

The policy will be communicated to staff / pupils / community in the following ways:

- Policy to be posted on the federation website and stored on the shared network drive
- Policy to be part of the induction pack for new staff
- E-safety to be discussed with pupils at the start of each year

Handling complaints

The federation will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the federation nor the local authority can accept liability for material accessed, or any consequences of internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - informing parents or carer
    - removal of internet or computer access for a period
    - referral to local authority / police
- All complaints should follow the school's agreed complaints procedure (available through the school website)
- Complaints of cyberbullying are dealt with in accordance with our anti-bullying policy. Complaints related to child protection are dealt with in accordance with school / local authority child protection procedures

Review and Monitoring

The e-safety policy will be referenced from within other school policies: child protection, anti-bullying and behaviour.

- The school has an information and communications technology (ICT) coordinator who will be responsible for document ownership, review and updates
- The e-safety policy will be reviewed regularly or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the senior leadership team and approved by governors. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff

2: Education and curriculum

Pupil e-safety curriculum

This federation:

- Has a clear, progressive, e-safety education programme as part of the computing curriculum / personal social health education (PSHE) curriculum. This covers a range of skills and behaviours appropriate to their age and experience
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind pupils about their responsibilities with regards to e-safety
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in popups; buying on-line; on-line gaming / gambling

Staff and governor training

This federation:

- Ensures staff and governors know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff and governors on e-safety issues
- Provides, as part of the induction process, all new staff and governors with information and guidance on the e-safeguarding policy

Parent awareness and training

This federation:

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the e-safety policy to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information in school newsletters; on the school web site
    - Suggestions for safe internet use at home
    - Provision of information about national support sites for parents

3: Expected conduct and incident management

Expected conduct

In this federation, all users:

- Are responsible for using the school information and communications technology (ICT) systems in accordance with the e-safety policy which they will be expected to sign before being given access to school systems
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school. They will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking and using of images and on cyber-bullying

Staff

- Are responsible for reading the school's e-safety policy and using the school information and communications technology (ICT) systems accordingly, including the use of mobile phones, and hand-held devices

Pupils

- should have a good understanding of research skills and acting responsibly and safely online

Parents/carers

- Should provide consent for pupils to use the internet, as well as other technologies, as part of the e-safety parental consent form (see Appendices 1 and 2) at the time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident management

In this federation:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- Support is actively sought from other agencies as needed
- Monitoring and reporting of e safety incidents takes place in accordance with general data protection regulations (GDPR) and the school's safeguarding policy and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and audited and reported to the school's senior leaders and governors, as appropriate

- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- The police will be contacted if one of our staff or pupils receives online communication that is considered to be particularly disturbing or breaks the law

4: Managing the information and communications technology (ICT) infrastructure
Internet access, security (virus protection) and filtering
This federation:

- Has the educational filtered secure broadband connectivity
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- Ensures network health through use of anti-virus software
- Uses department for education approved methods to send personal data over the internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site
- Only unblocks other external social networking sites for specific purposes
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable
- Ensures all staff and students read and understand the e-safety policy and understand that they must report any concerns
- Ensures pupils only publish within an appropriate environment
- Informs all users that internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the information and communications technology (ICT) co-ordinator
- Immediately refers any material we suspect is illegal to the appropriate authorities: police and the local authority

Network management (user access, backup)
This federation:

- Uses individual, audited log-ins for all staff users
- Ensures storage of all data within the school conforms to the general data protection regulation (GDPR)

To ensure the network is used safely, this federation:

- Ensures staff read and accept the e-safety policy

Photographs and videos of children

- To comply with the Data Protection Act 1998, we ask for parents' permission before we photograph or make recordings of pupils
- The following rules are adopted for any external use of digital images:
    - Where a pupil is named, we avoid using their photograph and if their photograph is used, we avoid naming the pupil
    - Where showcasing examples of pupils' work, we only use their first names, rather than their full names

- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film
- Only images of pupils in suitable dress are used

5: Data security: management information system access and data transfer
Strategic and operational practices
In this federation:

- The executive headteacher is the senior information risk officer
- Staff are clear who are the key contact(s) for key school information (the information asset owners)
- We ensure staff know to whom to report any incidents where data protection may have been compromised
- All staff are disclosure and barring service (DBS) checked and records are held in one central record.
- Local authority guidelines are followed for the transfer of any data, such as management information system data or reports of children, to professionals working in the local authority or their partners in children's services
- Any protect and restricted material must be encrypted if the material is to be removed from the school and such data removal is limited. There is an approved remote access solution so staff can access sensitive and other data from home, without need to take data home

Technical solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs
- Protect and restricted written material is stored in lockable storage cabinets in a lockable storage area
- There is compliance with the waste electrical and electronic equipment (WEEE) directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held
- Paper based sensitive information is shredded, using cross cut shredders

6: Equipment and digital content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member or visitor's own risk. The federation accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school
- Any pupil bringing a mobile device into school must hand it in to the school office on arrival
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the executive headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary

Digital images and video

In this federation:

- Parental / carer permission is obtained for use of digital photographs or video involving their child as part of the parental consent form when their child joins the school
- Pupils are not identified in online photographic materials or the full names of pupils included in the credits of any published school produced video materials / digital video discs (DVDs)
- Staff read the e-safety policy which includes reference to the use of mobile phones / personal equipment for taking pictures of pupils
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term use
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their information and communications technology (ICT) scheme of work
- Pupils are taught that they should not post images or videos of others without their permission

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory
- Details of all school-owned software will be recorded in a software inventory
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Appendix 1: Parental Consent Form (St John's)

St John the Evangelist Infant and Nursery School

Old Newtown Road, Newbury, Berkshire RG14 7DE

PARENT/GUARDIAN'S CONSENT FORMS

CHILD'S NAME:

During your child's time at St John the Evangelist School there are a number of areas that require parental consent. **Please read, sign and date each section below and return to the school office as soon as possible**.

Section 1: Local off site consent

The children are often given the opportunity to undertake activities/visits to local venues such as St John's Church, Victoria Park, Newbury Museum, and Newbury Library etc. Local, in this instance means in or around Newbury which will not require transportation. You will be informed at least 2 days before any such off site activity takes place.

I give permission for my child to take part in all such local off site activities during their time at St John the Evangelist School.

Signed: …….. (Parent's signature) Date: ……

Section 2: Web publication of work

I agree that, if selected, my child's work may be published on the school website whilst my child attends the school.

Signed: …….. (Parent's signature) Date: …….

Section 3: Using images of children

There are times when we invite the media into school to take photographs or film footage of a visiting dignitary or other event (school fete, play etc.) Pupils will often appear in these images, which may then appear in local or national newspapers, or on televised news programmes.

We also like to include photographs of the children in our own displays, website, social media (Facebook) page (private – for current parents only), prospectus and other material produced by the school. There are also occasions, such as assemblies/productions, when we may video the children's performances or use webcam for school to school conferences, monitoring or other educational use.

To comply with the Data Protection Act 2018, we need your permission before we can photograph or make any recordings of your child. Please answer the following questions by circling your answer and sign the form below where shown:

1. May we use your child's photograph in the school prospectus and other school publications/displays? YES / NO

2. May we use your child's photograph on our website? YES / NO

3. May we use your child's photograph on our private social media (Facebook) page? YES / NO

4. May we record your child's image on video or webcam e.g. for end of term videos and virtual performances? YES / NO

5. Are you happy for your child to appear in the media? YES / NO

6. Do you agree to your child's image being taken by our school photographer for class or group photograph's, which may then be distributed to other parents of pupils within the class/group? YES / NO

Please note: If you do not give permission then your child will not be included in class or group photographs

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Please also note that the **conditions for use** of these photographs are as follows:

1. This consent is valid for four years from the date signed, or for the period of time your child attends this school **unless you notify us** (in writing) **otherwise**. The consent will automatically expire after this time.

2. We will not re-use any photographs or recordings after your child leaves this school.

3. We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image or on video, on our website or social media page, in our school prospectus or in any other printed publications.

4. We will not include personal email or postal addresses, or telephone or fax numbers on video, on our website or social media page, in our school prospectus or in other printed publications.

5. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.

6. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

7. We may include pictures of pupils and teachers that have been drawn by the pupils.

8. We may use group or class photographs or footage with very general labels, such as 'science lesson' or 'making Christmas decorations'.

9. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

There may be opportunities, such as sport's days, Nativity plays etc, where you may wish to photograph your child.

As the child's parents/guardians, we agree that if we take photographs or video recordings of our child/ren which include other pupils, we will:

*Use these for personal and family use only

*Only put photos of our children taken at school on social media networks if they do not contain recognisable images of other children

I/we understand that where consent has not been obtained from the other parents for any other use, I/we would be in breach of the Data Protection Act 1998 if we used our images or recordings for any wider purpose.

I have read and understood the conditions of use as set out above:

Signed: …….. **(Parent's signature) Date:** …….

Section 4: Pupil Internet Access

As part of pupils' curriculum entitlement and the development of ICT skills, St John the Evangelist School provides supervised access to the Internet. Pupils will be able to exchange electronic mail with partner schools and research information from museums, libraries, news providers and suitable web sites as part of their programme of learning. All screens are in public view and access will be supervised.

I give permission for my child to access the Internet whilst attending St John the Evangelist School. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of Internet facilities.

Signed: …… (Parent's signature) Date: ……

Section 5: Change of clothes

There are occasions when children will need to change their clothes under the supervision of a member of staff.

I give permission for my child's clothes to be changed by a member of staff.

Signed: …….. (Parent's signature) Date: …….

Appendix 2: Parental consent form (St Nic's)

St Nicolas CE Junior School

Link Road, Newbury, Berkshire RG14 7LU

PARENT/GUARDIAN'S CONSENT FORMS

CHILD'S NAME:

During your child's time at St Nicolas School there are a number of areas that require parental consent. **Please read, sign and date each section below and return to the school office as soon as possible**.

Section 1: Consent for Local Visits

Throughout the year the school organises a number of visits and journeys away from the school site as part of the children's learning experiences. Such visits take place during the school session times and tend to be local to the school area. These trips are on foot and do not require transportation.

Visits and journeys during the school day are an extension to their classroom activities and present no significant risk to the health and safety of the pupils. All visits and journeys away from the school site must be approved by the Headteacher.

The purpose of this consent is to enable parents/guardians of children at the school to give their permission for their child to participate in frequent, local, curriculum focussed visits and journeys away from the school during the school day. This consent will allow your child to leave the school site for a local visit on several occasions without having to sign a separate consent form for each visit. You will not necessarily be advised in advance of these trips.

Examples of such visits are: Local sports fixtures both during school hours and at set after school times; Local visits to the local park, museums, churches, libraries, woodlands and other local used outdoor sites, etc; Town/village walks and the immediate countryside.

I have read this form and understand that I am only giving my consent to allow my child to participate in routine visits and journeys which take place during school times as an extension of their curriculum activities. I understand that all such visits and journeys have been risk assessed, have been approved by the Headteacher, and follow the Local Authority's guidance.

Signed: …… Date ……

Section 2: Films and Video Clips

At various times throughout the year we allow the children to watch films to further enhance the curriculum, or as a treat. The films are suitable for all ages or PG. All films are vetted by staff to make sure they are suitable before being shown. We would like your permission to be able to allow your child to watch PG films in school.

Additionally, class teachers may at times use clips of programmes from Internet sites, including BBC iPlayer or ITV Player. These clips are always watched by members of staff first and will always be related to curriculum areas, including the International Primary Curriculum. Sometimes, the shows will have been originally broadcast after the 9pm watershed. If this is the case, staff will ensure that the clips are appropriate to the age group of the children.

I give permission for my child to watch a PG rated film/video clip in school.

Signed: ……Date
……..

Section 3: Images of Children

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child **and there is a legal obligation for the school to hold a record.** Please answer questions 1 to 3 below, (delete as applicable), then sign and date where shown.

1. May we use your child's image on our official school website? **Yes / No**

2. May we use your child's image on our official St John & St Nicolas School Federation Facebook page, e.g. when
children are on a school trip or taking part in any activities in school. Your child's name will not appear with the image. **Yes / No**
3. Do we have your permission for your child to be photographed by the media and potentially appear on their websites? e.g. Newbury Weekly News, Sporting events, Y6 Moving Up Photo **Yes / No**

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies. Please also note that the conditions for use of these images are as follows:

Conditions of use
This form is valid for five years from the date you sign it, or until one year after your child leaves this school unless you notify us otherwise. The consent will automatically expire after this time.
We will not re-use any photographs or recordings beyond the period of consent.

We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website or in any of our other printed publications.

We will not include personal e-mail, postal addresses, or telephone numbers on video, on our website, or in other printed publications.

If we use photographs of individual pupils, we will **NOT** use the name of that child in the accompanying text or photo caption, except where access is restricted to the school community i.e. pupils, teachers and pupils' parents or guardians, or within school premises.

If we name a pupil in the text, we will not use a photograph of that child to accompany the article, except where access is restricted to the school community i.e. pupils, teachers and pupils' parents or guardians, or within school premises.

We may include pictures of pupils and teachers that have been drawn by the pupils.

We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".

Where showcasing examples of pupils work we only use their first names, rather than their full names.

Section 4: Acceptable ICT Use Policy for Pupils

Aims:

- **To allow all users to access and use the School Network and the Internet for educational purposes;**
- **To provide a system by which staff and pupils are protected from sites, information and individuals which would undermine the principles and aims of the school;**
- **To provide rules which are consistent and in agreement with the Data Protection Act;**
- **To provide a framework of rules which are consistent with the acceptable procedures commonly used on the Internet and School Network;**
- **To ensure accountability for any breach of the rules.**

Conditions:

You must obtain permission from a staff member before you can be allowed to use the School Network or Internet;
You must only access sites and services you have been given permission to use;
I know that accounts on some websites and social networks, such as Facebook, are not available for children at primary school.
You must not use the Internet without permission from a staff member;
Do not disclose any password or log-in details to anyone;
Do not give out personal details over the Internet;
Do not download, use or upload any material without permission from a staff member;
I will only edit or delete my own files and not look at, or change, other people's files without their permission
If I see anything I am unhappy with I will turn off my screen and tell a teacher or another adult in school.
If I receive a message I do not like, I will not respond to it but I will show a teacher / another adult in school.
Always respect the privacy of files of other users;
Be polite and respect other people's views. The use of strong or inappropriate language or aggressive behaviour is not allowed. This applies generally, but also in stored work, emails or the school website;
Make sure you log off when you have finished using a computer;
Portable storage devices, i.e. CDs, DVDs, USB memory sticks, should not be brought to school without parental permission and we cannot accept responsibility for their safekeeping. It is preferable to use email;
Report any incident which breaches the Acceptable Use Policy to the ICT staff;
We discourage mobile telephones being brought into school. However, if you consider that your child needs a phone, it must be named, switched off and handed to the class teacher at the beginning of the day; then collected at the end of the day. The school takes no responsibility for lost or damaged phones, or failure of pupils to remember to take them home.

Failure to comply with these rules will result in one or more of the following:
(i) A ban, temporary or permanent, on the use of the School Network or Internet facilities;
(ii) A letter informing your parents of the nature and breach of rules;
(iii) Appropriate sanctions and restrictions placed on access to school facilities;
(iv) Any other action decided by the Headteacher and Governors of St Nicolas C of E Junior School.

Declaration:
I understand and agree to abide by the conditions of this policy.
I understand that any breach of the conditions may result in disciplinary action.
I agree to report any misuse of the system to the ICT staff.

Child's Name: ……. Signed by Child: …….

Parent/Carer's Name: …… Signed by Parent/Carer :……

Date: ……

I have read and understood the conditions of use.

Signed: …… Date: ……

Section 5: Social Networking and online Media

I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Parent/Care's Name: …… Date: ……

Pupil Online Safety

These rules and promises will keep me safe and help me to be fair to others.

I promise to **THINK** about what I write or say online. I promise that what I write will be:

- **T**rue.
- **H**elpful**.**
- **I**nspiring**.**
- **N**ecessary**.**
- **K**ind. If not, then **STOP**!

I know that bullying can happen on the internet (cyber-bullying) just like it can in other places. I will remember to use **STOP** to remind me to Start Telling Other People if I am worried about cyber-bullying.

When working, playing or learning online, I promise to be **SMART:**

- **Stay** safe: Don't give out personal information to people you don't know.
- Don't **Meet** up: Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.
- **Accepting** files: Accepting emails, files or pictures from people you don't know can cause problems.
- **Reliable**: Check information before you believe it.
- **Tell** someone: tell an adult if someone or something makes you feel worried or uncomfortable.

As part of our anti-bullying policy, we take cyber-bullying very seriously. Cyberbullying is when a child receives unkind messages or experiences other behaviour online that occurs Several Times on Purpose.

If worried children should **STOP**:

- **S**tart
- **T**elling
- **O**ther
- **P**eople

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.
In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. (All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

I have read and understand these rules and promises and agree to them.

Child's Name: ……. Signed: …….

Date: …….