



# Online Safety Policy

---

**St. Francis' College**

September 2024

## Contents

Introduction.....	3
Policy .....	3
The key categories of risk.....	3
Legislation and guidance .....	3
Roles and responsibilities.....	4
Inspired Learning Group (ILG) .....	4
The Head .....	4
The Designated Safeguarding Lead .....	4
The ICT Manager .....	4
All staff and volunteers .....	5
Parents .....	5
Visitors and members of the community.....	6
Educating pupils about online safety .....	6
Educating parents about online safety .....	7
CYBERBULLYING: .....	7
Preventing and addressing cyber-bullying .....	8
Examining electronic devices .....	8
Acceptable use of the internet in College.....	9
Pupils using mobile devices in College .....	9
Staff using work devices outside College .....	9
How the College will respond to issues of misuse .....	10
Training.....	10
Monitoring arrangements .....	11
Related Policies .....	11
Version Control.....	11
Appendix 1.....	12
Appendix 2.....	13
Appendix 3.....	14
Appendix 4.....	15
Appendix 5.....	<u>17</u>

## Introduction

The 'College' refers to all the staff and pupils of the Prep Department and Senior School which includes Early Years Foundation Stage (EYFS), Pre-prep (Key Stage 1), Prep (Key Stage 2), and Senior School (Key Stages 3-5).

## Policy

Our College aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Inspired Learning Group (ILG)
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## The key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to:

- DfE's guidance on protecting children from radicalisation.
- Searching, Screening, and Confiscation (DfE, July 2023)

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

## **Roles and responsibilities**

### **Inspired Learning Group (ILG)**

Inspired Learning Group retains overall responsibility for holding the Head accountable for compliance with this policy.

### **The Head**

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

### **The Designated Safeguarding Lead**

Details of the College's DSL and DDSLs are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in College, in particular:

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the College
- Working with the Head, ICT Provider and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the College Child Protection Policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College Behaviour Policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to the Head and/or ILG

This list is not intended to be exhaustive.

### **The ICT Manager**

The ICT Provider is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College Behaviour Policy

This list is not intended to be exhaustive.

### **All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the College's ICT systems and the internet (appendix 3), and ensuring that pupils follow the College's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

### **Parents**

Parents are expected to:

- Notify a member of staff or the Head of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the College's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

## Visitors and members of the community

Visitors and members of the community who use the College's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

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

By the end of primary school, pupils will know:

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

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in ICT, Personal Development and other subjects where relevant. Safe use of social media and the internet is also covered during form time and assemblies.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

### **Educating parents about online safety**

The College will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during the New Academic Year Induction Evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Designated Safeguarding Lead, who is also the Assistant Head Pastoral.

### **CYBERBULLYING:**

#### **Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See also the College Behaviour and Discipline Policy.

### **Preventing and addressing cyber-bullying**

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

The College will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups.

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

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

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the College will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

### **Examining electronic devices**

College staff have the specific power under the Education Act 2011 to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police\*



\* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the College complaints procedure.

### **Acceptable use of the internet in College**

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

Use of the College's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, ILG and visitors (where relevant) to ensure they comply with the above.

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

### **Pupils using mobile devices in College**

Pupils may bring mobile devices into College but are not permitted to use them during the school day (8.30am - 4pm). Sixth formers may use their devices in the Sixth form area only.

Any use of mobile devices in College by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

### **Staff using work devices outside College**

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

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

Work devices must be used solely for work activities.

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

### **How the College will respond to issues of misuse**

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

Where a staff member misuses the College's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

### **Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse. Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptom of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

### **Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with ILG.

### **Related Policies**

Safeguarding Policy  
Behaviour policy  
Disciplinary Policy - Staff  
Data Protection Policy  
Privacy Policy  
Complaints Procedure  
Acceptable Use Policy

### **Version Control**

Reviewed By	Assistant Head Pastoral
Authorised By	Head
Effective From	September 2024
Next Review Due	September 2026

## Appendix 1

### EYFS and KS1 acceptable use agreement (pupils and parents/carers)

#### ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

**When I use the College's ICT systems (like computers) and get onto the internet in College I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use College computers for College work only
- Be kind to others and not upset or be rude to them
- Look after the College ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/guardian
- Save my work on the College network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

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

Signed (pupil):

Date:

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

Signed (parent/guardian):

Date:

## Appendix 2

### KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

#### ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the College's ICT systems (like computers) and get onto the internet in College I will:**

- Always use the College's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the College's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**If I bring a personal mobile phone or other personal electronic device into College:**

- I will not use it during lessons, tutor group time, clubs or other activities organised by the College, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

Signed (pupil):

Date:

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

Signed (parent/guardian):

Date:

### Appendix 3

#### Acceptable use agreement (staff, ILG, volunteers and visitors)

#### ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, ILG, VOLUNTEERS AND VISITORS

**Name of staff member/ILG/volunteer/visitor:**

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

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

- I will only use the College's ICT systems and access the internet in College, or outside College on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the College will monitor the websites I visit and my use of the College's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside College, and keep all data securely stored in accordance with this policy and the College's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the College's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/ILG/volunteer/visitor):**

**Date:**

## Appendix 4

### Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
<b>Question</b>	<b>Yes/No (add comments if necessary)</b>
Do you know the name of the person who has lead responsibility for online safety in College?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the College's acceptable use agreement for staff, volunteers, ILG and visitors?	
Are you familiar with the College's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the College's ICT systems?	
Are you familiar with the College's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

**Appendix 5**

**Online Safety Incident Log**

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident