



Kick Start Futures

Online Safety Policy

Connect • Create • Think • Stay Safe

Policy Date: August 2026

Review Date: August 2027

1. Policy Statement

Digital technology is an important part of young people's education, relationships and everyday lives.

At Kick Start Futures, we want students to develop the skills to use technology **safely, responsibly and confidently**, rather than simply trying to remove every online risk.

Online safety is also a safeguarding responsibility.

The risks young people experience online can affect their wellbeing, relationships and safety both inside and outside KSF.

Our approach therefore combines:

education • appropriate boundaries • supervision • safeguarding • responsibility

Where something goes wrong online, we will seek to protect those affected, understand what has happened and help students make safer choices in the future.

2. Purpose

This policy aims to:

- safeguard students from online harm;
- promote safe and responsible use of technology;
- establish clear expectations for students and staff;
- ensure online safeguarding concerns are recognised and reported;
- address cyberbullying and harmful online behaviour;
- protect personal and confidential information;
- manage photography and social media safely;
- promote appropriate use of artificial intelligence;
- ensure suitable filtering and monitoring arrangements are in place;
- help young people develop the skills to manage online risks beyond KSF.

3. Online Safety and Safeguarding

Online safety forms part of KSF's wider safeguarding responsibilities.

Online risks may include:

- bullying and harassment;
- harmful or inappropriate content;
- sexual harassment;
- grooming;
- exploitation;
- coercion;
- scams and fraud;
- sharing intimate images;
- extremist content;
- misinformation;
- contact with unsafe individuals;
- excessive or harmful use of technology;

- risks associated with AI-generated content.

Staff must remain professionally curious when a student's online behaviour, relationships or experiences cause concern.

Concerns about a child's safety must be reported to the **Designated Safeguarding Lead (DSL)**.

4. Our Approach to Online Safety

Simply telling young people "**don't go online**" is neither realistic nor effective.

We want students to learn to:

- recognise risk;
- protect personal information;
- question what they see online;
- communicate respectfully;
- understand consent;
- recognise manipulation or grooming;
- know when and how to ask for help;
- understand that online actions can have real-world consequences.

Online safety education will be appropriate to students' age, understanding, SEND and individual vulnerability.

5. Student Use of Technology

Students may use KSF technology for agreed educational purposes.

Students are expected to:

- use equipment appropriately;
- follow staff instructions;
- keep passwords secure;
- respect other people's privacy;
- communicate respectfully;
- avoid accessing or attempting to access inappropriate material;
- report concerning content;
- avoid deliberately bypassing security or filtering systems;
- respect copyright and ownership of other people's work.

Where technology is misused, staff will respond proportionately in accordance with the **Relationships Policy**.

6. Personal Mobile Phones

KSF recognises that phones are an important part of everyday life and that a blanket approach may not be appropriate for every student.

Expectations for phone use will therefore be clear and proportionate.

Students may be asked to put phones away during:

- teaching;
- football coaching;
- group activities;
- restorative conversations;
- other times where phone use interferes with learning, relationships or safety.

Where a student needs access to a phone for an agreed medical, SEND, travel or safeguarding reason, appropriate arrangements can be made.

Persistent or unsafe phone use will be addressed individually.

7. Photography and Filming by Students

Students must not photograph, film or record another person without appropriate permission.

Recording is never acceptable in:

- toilets;
- changing rooms;
- private or sensitive conversations;
- situations where another person has asked not to be recorded.

Students must not use images or recordings to:

- humiliate someone;
- threaten or bully;
- create sexualised content;
- impersonate another person;
- share private information.

Serious concerns will be treated as safeguarding matters where appropriate.

8. Photography and Salisbury FC

KSF operates within a football stadium where photography, filming, media and social media activity may occur as part of normal club operations.

The presence of a KSF student at the stadium **does not automatically provide consent for their image to be photographed, filmed or published.**

KSF will maintain appropriate arrangements with Salisbury FC to protect students.

Where students are involved in photographs or filming for KSF or Salisbury FC purposes:

- appropriate consent arrangements must be followed;
- safeguarding information must be considered;
- students who should not be photographed must be protected;
- images must be used only for the agreed purpose.

KSF staff must remain alert during matches, events or other occasions where photographers or members of the public may be present.

9. Social Media

Students will be supported to understand that social media can create both opportunities and risks.

Education will include appropriate discussion of:

- privacy settings;
- location sharing;
- personal information;
- online reputation;
- respectful communication;
- fake accounts;
- scams;
- harmful content;
- grooming;
- sharing images;
- pressure from peers;
- permanence of online content.

KSF will not routinely monitor students' personal social media accounts.

However, where information is brought to our attention that raises a safeguarding concern or significantly affects students within KSF, we will respond appropriately.

10. Cyberbullying

Cyberbullying will be taken as seriously as bullying that occurs face-to-face.

This may include:

- abusive messages;
- threatening communication;
- spreading rumours;
- deliberately excluding someone from online groups;
- sharing embarrassing images or videos;
- impersonating another person;
- discriminatory abuse;
- repeated unwanted contact.

KSF may respond to online behaviour occurring outside provision hours where it affects the **safety, wellbeing or relationships of KSF students**.

Students experiencing cyberbullying will be encouraged, where safe, to preserve relevant evidence such as screenshots.

The **Anti-Bullying Policy** will also apply.

11. Sexualised Online Behaviour

Young people may encounter or become involved in sexualised behaviour online.

This can include:

- sexual messages;
- requests for images;
- sharing intimate images;
- unwanted sexual comments;
- pressure or coercion;
- sexualised group chats;
- sharing pornography;
- AI-generated sexualised images.

Staff must not dismiss these concerns as experimentation, joking or normal teenage behaviour without considering the circumstances and safeguarding implications.

Concerns will be reported to the DSL and managed in accordance with current safeguarding procedures.

12. Sharing Intimate Images

Where staff become aware that a student may have created, requested, received or shared a nude or semi-nude image or video, the matter must be reported to the **DSL immediately**.

Staff must **not routinely view, copy, print, forward or save the image**.

The DSL will determine the appropriate safeguarding response in accordance with current guidance, considering:

- the age of those involved;
- consent;
- coercion;
- exploitation;
- whether the image has been shared further;
- vulnerability;
- risk of ongoing harm.

Students will be supported rather than shamed for reporting concerns.

13. Grooming and Exploitation

Staff should be alert to signs that a young person may be forming an unsafe online relationship.

Possible concerns may include:

- secretive communication;
- contact with significantly older individuals;
- unexplained gifts or money;
- pressure to meet someone;
- requests for sexual images;

- threats or blackmail;
- sudden changes in behaviour;
- involvement in criminal or sexual exploitation.

Staff should **not attempt to investigate suspected grooming themselves**.

Concerns must be reported promptly to the DSL.

14. Harmful and Inappropriate Content

Students may accidentally or deliberately encounter content involving:

- pornography;
- violence;
- self-harm;
- suicide;
- eating disorders;
- hate or discrimination;
- extremism;
- dangerous challenges;
- drugs;
- criminal activity.

Where this occurs, staff should respond calmly.

The response should consider:

- what was accessed;
- whether access was accidental or deliberate;
- the student's age and understanding;
- whether content has been shared;
- whether there is an immediate safeguarding risk;
- whether the behaviour indicates a wider concern.

Students should feel able to tell an adult when they have seen something disturbing without automatically fearing punishment.

15. Staff Online Conduct

Staff must maintain professional boundaries online.

Staff must not:

- add current students to personal social media accounts;
- privately message students through personal accounts;
- share personal contact details without appropriate authorisation;
- photograph students using personal devices;
- publish confidential KSF information;
- post identifiable information about students;
- engage in online behaviour that compromises their suitability to work with children.

Staff should assume that anything posted publicly may eventually be seen by students, families or colleagues.

Further expectations are contained within the **Staff Code of Conduct**.

16. Communication with Students

Electronic communication with students must take place through **approved KSF systems or specifically authorised arrangements**.

Communication should:

- have a legitimate professional purpose;
- be appropriate in tone;
- maintain professional boundaries;
- be capable of appropriate organisational oversight.

Staff should never establish secret or private channels of communication with students.

Where unusual circumstances require a different arrangement, this must be explicitly agreed with the Education & Provision Lead.

17. Passwords, Accounts and Data

Staff and students are expected to protect accounts and personal information.

Staff must:

- use secure passwords;
- keep login information confidential;
- lock devices when unattended;
- avoid accessing confidential information in public areas;
- use approved systems for student information;
- report suspected data breaches promptly.

Student information must not be stored on personal devices unless specifically authorised and appropriately secured.

18. Filtering and Monitoring

KSF will have appropriate arrangements to reduce the risk of students accessing harmful or inappropriate online content.

Filtering and monitoring arrangements will be proportionate to the provision and the needs of its students.

KSF will ensure that:

- appropriate internet filtering is in place;
- filtering does not unnecessarily restrict legitimate educational content;
- concerns identified through monitoring are acted upon;
- staff understand their role in monitoring student internet use;
- arrangements are reviewed regularly.

Filtering systems are an important safeguard, but they **do not replace staff supervision, professional curiosity or online-safety education**.

19. Salisbury FC Wi-Fi and IT Systems

Where KSF uses internet or IT infrastructure provided by Salisbury FC, responsibilities for filtering, monitoring and technical security will be clearly agreed between the organisations.

KSF will satisfy itself that the internet access used by students provides appropriate safeguarding controls.

If existing Salisbury FC systems do not provide the level of filtering or monitoring required for KSF students, additional arrangements will be introduced.

Staff should report concerns about filtering, inappropriate access or network security promptly.

20. Artificial Intelligence

Artificial intelligence can provide useful opportunities for learning, creativity and preparation for future employment.

Students may use approved AI tools for legitimate educational purposes with appropriate staff guidance.

Students will be taught that AI-generated information can be:

- inaccurate;
- biased;
- misleading;
- fabricated;
- inappropriate;
- based on unreliable information.

Students should not use AI to:

- bully or humiliate others;
- create harmful or sexualised images;
- impersonate another person;
- create discriminatory content;
- deceive staff about their work;
- share another person's private information.

Staff remain responsible for checking the accuracy and appropriateness of AI-generated materials they use professionally.

21. Confidential Information and AI

Staff must **not enter identifiable, confidential or sensitive information about students, families or colleagues into publicly available AI systems** unless the system has been specifically approved for that purpose and appropriate data protection arrangements are in place.

This includes information from:

- EHCPs;
- safeguarding records;
- student reports;
- medical information;
- behaviour or incident records;
- personal correspondence.

Where AI is used to support professional tasks, information should be anonymised where appropriate and staff remain responsible for the final content.

22. Deepfakes and Manipulated Content

Developments in AI mean that images, video, audio and written content can increasingly be manipulated or fabricated.

Students will be supported to understand:

Seeing something online does not automatically mean it is real.

Creating or sharing manipulated content to bully, humiliate, sexually exploit, threaten or impersonate another person will be treated seriously.

Where manipulated sexual images of a child are involved, the matter will be treated as a safeguarding concern and referred immediately to the DSL.

23. Misinformation and Digital Literacy

KSF will help students develop critical digital literacy.

Students will be encouraged to ask:

- Who created this?
- Why was it created?
- Is the source reliable?
- Can the information be checked elsewhere?
- Is somebody trying to influence my emotions?
- Could this image, video or account be fake?

The aim is not to tell students **what to think**, but to help them learn **how to question what they see**.

24. Online Radicalisation and Extremism

The internet can be used to expose young people to extremist material or attempt to influence and radicalise them.

Staff should remain alert to concerning changes in:

- online interests;
- language;
- attitudes;

- relationships;
- content being shared or accessed.

A student expressing a controversial or challenging opinion does not automatically indicate radicalisation.

Concerns should be considered in context and reported to the DSL where there is a safeguarding concern.

KSF will follow its safeguarding procedures and statutory **Prevent** responsibilities where applicable.

25. SEND and Online Vulnerability

Some students with SEND may experience additional online vulnerabilities.

These can include difficulty:

- recognising manipulation;
- interpreting another person's intentions;
- understanding privacy;
- recognising scams;
- understanding appropriate boundaries;
- managing impulsive online behaviour;
- communicating that something unsafe has happened.

Online-safety education and support will therefore be adapted to the individual student's needs and understanding.

Staff must avoid assuming that a student understands online risks simply because they can use technology confidently.

26. Responding to an Online Safety Incident

Where an online-safety incident occurs, staff should:

1. **Make safe** – consider whether anyone is at immediate risk.
2. **Preserve appropriate evidence** – where necessary and safe to do so.
3. **Report** – inform the DSL where there is a safeguarding concern.
4. **Do not investigate beyond your role** – particularly where criminal or sexual harm may be involved.
5. **Support** – ensure affected students receive appropriate support.
6. **Review** – consider whether additional safeguards, education or changes are required.

Where appropriate, parents/carers, commissioning schools, Police or other agencies may be involved.

27. Searching or Confiscating a Device

There may be circumstances where staff have concerns about content on a student's device.

Staff should **not routinely search through a student's personal phone or accounts themselves**.

Any decision to search, examine or confiscate a device must be lawful, proportionate and consistent with KSF procedures and current guidance.

Where there is concern about sexual images, criminal activity, exploitation or another serious safeguarding matter, staff should seek advice from the DSL before accessing content wherever possible.

A device may need to be secured while appropriate advice is obtained.

28. Online Incidents Outside KSF

KSF recognises that much of students' online activity occurs outside provision hours.

We will not attempt to police students' private lives.

However, KSF may become involved where online behaviour:

- creates a safeguarding concern;
- affects relationships within KSF;
- involves cyberbullying between students;
- threatens another student or member of staff;
- involves harmful sexual behaviour;
- significantly affects a student's ability to participate safely in the provision.

Our response will focus on **safety, education, responsibility and repair**.

29. Working with Parents and Carers

Families play an important role in online safety.

Where appropriate, KSF will work with parents/carers to:

- share concerns;
- provide information about emerging risks;
- support appropriate boundaries;
- address cyberbullying;
- respond to safeguarding incidents;
- encourage open conversations about online activity.

We recognise that technology changes quickly and that adults will not always know every app, platform or trend being used by young people.

The most important protective factor is often that a young person feels able to **tell a trusted adult when something goes wrong**.

30. Working with Commissioning Schools

Where an online incident involves a student who remains on the roll of another school, KSF will communicate appropriately with the commissioning school.

This is particularly important where:

- students from different provisions are involved;
- safeguarding concerns arise;
- behaviour occurs across school and KSF;
- ongoing support is required;
- risk assessments or safety plans need to be reviewed.

Safeguarding information will be shared promptly where necessary to protect a child.

31. Staff Training

Staff will receive appropriate online-safety information through induction and ongoing safeguarding training.

Training will reflect emerging risks and may include:

- cyberbullying;
- social media;
- grooming and exploitation;
- online sexual harm;
- sharing intimate images;
- filtering and monitoring;
- radicalisation;
- AI and deepfakes;
- professional online boundaries.

Staff do not need to be technology experts.

They **do** need to recognise when something may be unsafe and know how to report it.

32. Responsibilities

Education & Provision Lead

The Education & Provision Lead will ensure that:

- this policy is implemented;
- appropriate filtering and monitoring arrangements are maintained;
- staff understand their responsibilities;
- significant concerns are reviewed;
- arrangements with Salisbury FC are appropriate;
- emerging online risks are considered.

Designated Safeguarding Lead

The DSL will:

- oversee safeguarding responses to online concerns;
- ensure appropriate referrals are made;
- advise staff on safeguarding risks;
- consider patterns and emerging concerns.

Staff

All staff will:

- model responsible technology use;
- supervise students appropriately;
- maintain professional online boundaries;
- report concerns promptly;
- follow KSF safeguarding procedures.

Students

Students will be encouraged to:

- use technology responsibly;
- respect other people online;
- protect personal information;
- report harmful content or contact;
- ask for help when something goes wrong.

33. Monitoring and Review

KSF will regularly consider whether its online-safety arrangements remain effective.

This will include reviewing:

- safeguarding incidents;
- filtering and monitoring;
- student behaviour and emerging risks;
- staff feedback;
- student voice;
- technological developments;
- arrangements with Salisbury FC.

Filtering and monitoring arrangements will be reviewed **at least annually**, and sooner where concerns or significant changes arise.

This policy will be reviewed annually or sooner following significant changes to legislation, statutory safeguarding guidance or technology.

34. Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Staff Code of Conduct;
- Relationships Policy;
- Anti-Bullying Policy;
- Low-Level Concerns Policy;
- Data Protection Policy;
- SEND Policy;
- Equality, Diversity & Inclusion Policy;
- Health & Safety Policy.

35. Our Commitment

Technology should open doors for young people, not simply create risks.

At Kick Start Futures, our aim is to help students become **confident and responsible digital citizens** who understand that the choices they make online affect themselves and other people.

We cannot remove every online risk.

We can give young people the **knowledge, relationships and confidence to recognise risk and ask for help when they need it.**

Our message is simple:

Think before you share.
Respect people online.
Question what you see.
Protect your information.
Tell someone when something doesn't feel right.

Connect • Create • Think • Stay Safe