Online Safety Policy

Reviewed by the Standards and Curriculum Committee	**Autumn 2025**
Adopted by the Governing Body	**Autumn 2025**
To be Reviewed:	**Autumn 2026**

CONTENTS

'In the light of Christ we will shine together'

Jesus said: I am the light of the world. John 8.12
Live as children of light – for the fruit of light is all that is good and true and right. Ephesians 5.8-9

Our ambition is to serve our community by providing an excellent education, which is inclusive and distinctive within the context of Christian belief and practice, upholding our values in the daily life of the Academy and in our relationships with others.

1. AIMS

1.1. The Academy aims to ensure that it will:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2. The 4 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, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer 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 scams

2. LEGISLATION AND STATUTORY GUIDANCE

2.1. 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

2.2. It also refers to the DfE's guidance on protecting children from radicalisation.

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.

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

2.4. This policy complies with our funding agreement and articles of association.

3. ROLES AND RESPONSIBILITIES

3.1. The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Governing Body will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

A named Governor will oversee online safety.

All Governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3) and the academy ICT and Acceptable Use policy.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- Complete the National Online Safety certified Online Safety Course for School Governors every 2 years.

3.2. The Principal

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

3.3. The Designated Safeguarding Lead

Details of the Academy's DSL and deputies are set out in our Safeguarding and Child Protection Policy.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the Principal, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the Academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or Governing Body
- Regularly reviewing the filtering and monitoring system - alerts are routed to an appropriate member of staff and acted upon as necessary.

This list is not intended to be exhaustive.

3.4. The ICT Manager

The ICT manager 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 school, including terrorist and extremist material
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Continually conducting security checks and monitoring the Academy's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and shared with the DSL

This list is not intended to be exhaustive.

3.5. All Staff and Volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the Internet , and ensuring that pupils follow the Academy's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the Academy 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.

In addition to the above, all teaching, support and admin staff will complete The National College Certificate in Online Safety for School Staff online.

3.6. Parents and Carers

Parents are expected to:

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

Parents and carers are encouraged to access and complete The National College Award in Online Safety for Parents.

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
- The National College
- The National College #WakeUpWednesday Parent and Educator guides

3.7. Visitors and Members of the Community

Visitors and members of the community who use the Academy'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).

Where a visitor comes in to deliver an assembly or presentation using ICT equipment to children, a member of staff must remain with the visitor whilst the presentation is delivered.

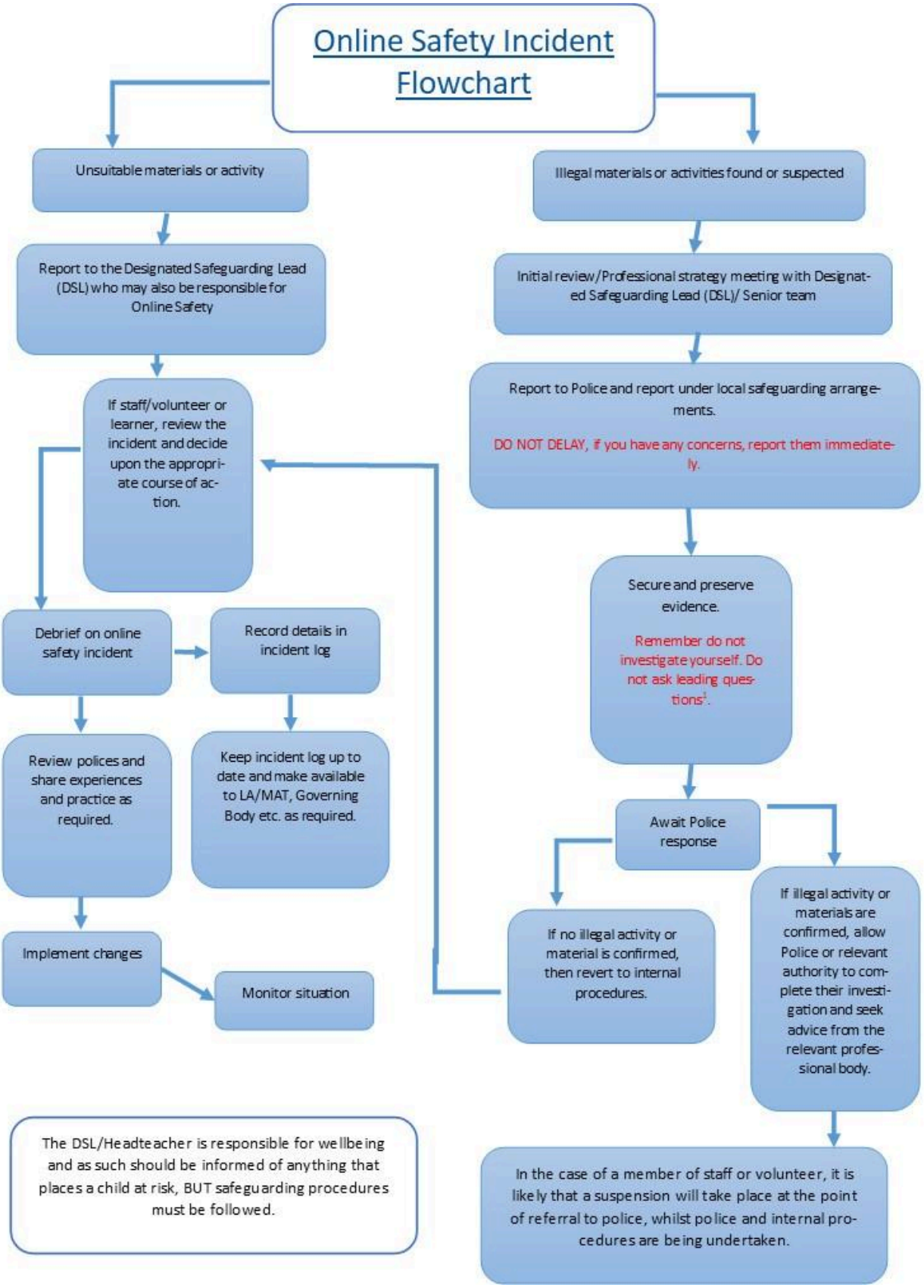
4. REPORTING AND RESPONDING TO ONLINE SAFETY INCIDENTS

4.1. The Academy will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart below), the incident must be escalated through the agreed school safeguarding procedures.
- Any concern about staff misuse will be reported to the Principal, unless the concern involves the Principal, in which case the concern is referred to the Chair of Governors and the local authority.
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- Incidents should be logged using the CPOMS reporting system.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Staff and children are aware that we use Securas to monitor online safety, checked daily by the DSL. Staff misuse will be stored on Staff Safe (CPOMS).
- Staff know that we use SurfProtect as our filtering software.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

    > staff, through regular briefings
    > learners, through assemblies/lessons
    > parents/carers, through newsletters, school social media, website
    > governors, through termly safeguarding updates
    > local authority/external agencies, as relevant

4.2. The Academy will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes
Monitor situation
Illegal materials or activities found or suspected
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

4.3. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures outlined in 'Our Good Behaviour Promise.

5. EDUCATING PUPILS ABOUT ONLINE SAFETY

5.1. In order to go online at school, pupils must read and agree to the acceptable use policy for their key stage annually. In addition, each class will discuss and write their own set of rules for being safe online at the start of every academic year which will be on display in the classroom and shared with parents and carers.

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

5.3. All schools have to teach:

- Relationships education and health education in primary schools

5.4. 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, contact or conduct on the internet or other online technologies.

5.5. 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, contact and conduct

5.6. 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.

5.7. The safe use of social media and the Internet will also be covered across a range of curriculum subjects where relevant.

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

5.9. Guidance on relationships education, relationships and sex education (RSE) and health education states that all schools have to teach relationships education and health education in primary schools in which elements of online safety will also be covered.

5.10. The Academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5.11. Teachers will work with the Online Safety Lead to develop a planned and coordinated online safety education programme through the use of Kapow, which fulfils the statutory requirements for computing outlined in the National Curriculum (2014) and, when used in conjunction with our RSE & PSHE scheme, also covers the government's Education for a Connected World 2020 edition framework.

5.12. The framework comprises eight strands of learning:

- Self-image and identity;
- Online relationships.
- Online reputation.
- Online bullying.
- Managing online information.
- Health, wellbeing and lifestyle.
- Privacy and security.
- Copyright and ownership.

5.13. In addition to distinct lessons, Online Safety will be addressed through selected PSHE units from Jigsaw: The Mindful Approach to PSHE.

5.14. Teachers will use our Insight Tracking assessment system to assess children's knowledge and understanding of online safety. This will be reported through the safeguarding link governor role. Where we have concerns about a child's understanding, additional support will be put in place.

6. EDUCATING PARENTS ABOUT ONLINE SAFETY

6.1. The Academy will raise parents' awareness of Internet safety in weekly roundups sharing The National College #WakeUpWednesday resource and through information published on our website. This policy will also be shared with parents. Email updates will be sent home as and when it is felt necessary as part of our ongoing reflections.

6.2. Online safety will also be covered during parents' welcome evenings at the start of the academic year.

6.3. Parents are encouraged to access The National College Award in Online Safety for Parents.

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

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

7. CYBERBULLYING

7.1. Definition

Cyberbullying 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.

7.2. Preventing and Addressing Cyberbullying

To help prevent cyberbullying, 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 Academy will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyberbullying with their classes, and the issue will be addressed in assemblies as well as the annual Anti-Bullying Week.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

The Academy also sends information/leaflets on cyberbullying 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 cyberbullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy 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.

7.3. Examining Electronic Devices

The Principal, and any member of staff authorised to do so by the Principal, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or

- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- **Cause harm, and/or**
- **Undermine the safe environment of the school or disrupt teaching, and/or**
- **Commit an offence**

If inappropriate material is found on the device, it is up to the Principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening 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 school complaints procedure.

8. ACCEPTABLE USE OF THE INTERNET AT THE ACADEMY

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

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

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

9. PERSONAL SMART DEVICES AT THE ACADEMY

9.1. Pupils - Mobile Phones in Years 5 & 6

Parents/carers of children in years 5 or 6 can decide if a pupil needs their phone for the journey to and from school. Mobile phones must be switched off before entering the school site (the blue gates) and be out of sight i.e. in bags or coat pockets. Once in class, they must be handed in to an assigned adult to be locked away for the day.

Parents and carers should be aware that The Academy accepts no liability for the loss or damage to any mobile phones or any other 'SMART' device, which are brought onto the school grounds, therefore they should make their own arrangements if they require insurance protection.

9.2. Smart Watches

Although we encourage children to wear basic analogue or digital watches in school, we do not allow children to wear a 'smart' watch, or any other watch that has the same functionality as a mobile phone or PC, on the school site.

If a pupil is found by a member of staff to be using a mobile phone or smart device at school, it will be confiscated from the pupil and handed to a member of staff, who will store it safely until the pupil collects it at the end of the school day. Should a pupil be found to be using a mobile phone or device again or inappropriately, then it will be confiscated and a member of the Senior Leadership Team will contact a parent/carer to collect the phone from school.

The school reserves the right to say that a pupil will no longer be able to bring a mobile phone into school.

Phones must not be taken on school trips/visits.

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

9.3. Staff

In accordance with the Staff Code of Conduct, members of staff must switch off mobile phones in classrooms. Should they need to use phones during the teaching day, this must be done in the staff room or in cars, away from pupils.

Adults can wear smartwatches in school. As with mobile phones, these must not be used for messaging or recording during the teaching day. Email/text notifications should be silenced during directed hours.

Some members of staff need to use mobile phones in order to carry out their duties. This will be agreed with members of senior leadership.

Personal mobile phones or devices must not be used for taking photos of pupils, instead only academy owned and registered devices may be used.

9.4. Visitors

As with all visitors, for Safeguarding reasons, parents/carers are required to put away their mobile phones on arrival in the playground. Visitors must not use their mobile phones whilst in school, unless they receive permission beforehand from a member of the Senior Leadership Team.

10. STAFF USING PERSONAL SMART DEVICES & PHONES AT THE ACADEMY

10.1. 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 or when the device is unattended
- 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

10.2. Staff members must not use the device in any way which would violate the school's terms of acceptable use.

10.3. Work devices must be used solely for work activities.

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

11. HOW THE ACADEMY WILL RESPOND TO ISSUES OF MISUSE

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

11.2. Where a staff member misuses the Academy'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 Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

11.3. Breaches of this policy will be recorded on StaffSafe (CPOMS).

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

12. TRAINING

12.1. All new staff members will receive training, as part of their induction, on safe Internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation and will complete The National College Certificate in Online Safety for School Staff online.

12.2. All staff members will receive refresher training at least once each academic year by completing The National College Certificate in Online Safety for School Staff online as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

12.3. 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:
  - o Abusive, harassing, and misogynistic messages
  - o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - o 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 symptoms 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

12.4. The DSL and deputies will undertake additional child protection and safeguarding training, which will include online safety, at least every 2 years. They will update their knowledge and skills on the subject of online safety at regular intervals, and at least annually, including completion of The National College Safety Advanced Certificate in Online Safety for DSLs & Deputy DSLs course.

12.5. Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training and will complete the National Online Safety 'Online Safety of School Staff and Governors' certificated course biennially.

12.6. Volunteers will receive appropriate training and updates, if applicable.

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

13. MONITORING AND REVIEW ARRANGEMENTS

13.1. The Principal and DSL will monitor behaviour and safeguarding issues related to online safety using our CPOMS recording system.

13.2. The Principal/Designated Safeguarding Lead and Link Governor will be responsible for monitoring the implementation and effectiveness of this policy. It will be reviewed annually by the Standards and Curriculum Committee; or before at any time, if there is new relevant legislation or guidance.

Appendix 1:

Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

I have read (or they have been read to me) and understand the rules above. I agree to follow them.

Signed (child): _____

Signed (parent): _____

Appendix 2:

Learner Acceptable Use Agreement Template – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programs.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will not use any personal devices in school.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, there will be logical consequences. This could include loss of access to the school network and internet, device privileges removed, parents/carers contacted and, in the event of illegal activities, involvement of the police.

Learner Acceptable Use Agreement Form:

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: _____ Group/Class:_____

Signed: _____ Date: _____

Parent Signature: _____

Appendix 3:

Staff and Governor - Acceptable use agreement /code of conduct

The school's acceptable use policy is designed to ensure that all staff are aware of their responsibilities when using any form of ICT within their professional role. It is compulsory for all staff to sign this document and adhere at all times to the contents every year.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role and never via personal email/phone accounts/social networking profiles. This must be done via the office.
- I will not discuss or post school issues on social media or refer to St Mary's Academy in name.
- I will not give out to pupils my own personal contact details – mobile phone number/personal email.
- I will only use the approved secure email service and VLE tools for communications related to my professional role.
- I am aware that communicating with parents/pupils via private social media/SMS etc may result in a disciplinary matter. I will make DSL /Head teacher aware if a pupil tries to contact me.
- I will regularly check my security settings and change if needed.
- I will ensure that personal data (such as the MIS system) is kept secure and is used appropriately, whether in school or accessed remotely.
- I will ensure if I take data off site it will be encrypted or accessed remotely.
- I will not install any hardware or software without permission of the ICT Lead.
- I will not browse, download, upload or distribute offensive, inappropriate or illegal material. I understand that to do so may be considered a disciplinary matter and in some cases a criminal offence.
- Images and videos of pupils/staff will only be taken and stored on school devices and will only be used for professional purposes, in line with school policy and parent/care consent.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity both in school and outside school, will not bring my professional role or that of the school into disrepute.
- I will support and promote the school's online safety policy and help pupils be safe and responsible in their use of ICT and other related technologies.
- I will follow school policies and legal requirements, with AI used responsibly for tasks like lesson planning and feedback under human oversight, while avoiding sharing personal data and plagiarism.

I agree to follow this code of conduct and support the safe use of ICT throughout the school.

Name: _____

Job Title: _____