E-Safety Policy September 2021

St John Fisher Catholic Voluntary Academy

Mission Statement

***'For I know the plans I have for you; plans to give you hope and a future**.'* Jeremiah 29:11

Policy Aims

This policy aims to:

- Set out expectations for all St John Fisher community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of todays and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world for the protection and benefit of the children and young people in their care, and or their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

The purpose of the e-safety policy.

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

The purpose of this policy is to ensure that all staff, parents, Directors and children understand and agree the Academy's approach to e-safety. The school's e-safety policy will operate in conjunction with other policies including those for email security, behaviour, anti-bullying, safeguarding, child protection, mobile phone, data protection, image consent form, ICT curriculum, internet access, and Health and Safety.

Writing and reviewing the e-safety policy

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Things may need changing in the light of potential closure, remote learning and alternative arrangements at school. Although many aspects will be informed by legislation and regulations, continue to involve staff, governors, pupils and parents in writing when reviewing the policy This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. The Academy will appoint an e-safety officer who will work closely with the DSL who will also be responsible for the online safety.

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct. Many of these new risks are mentioned in KCSIE 2021, e.g., extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, up skirting and sticky design e.g., Persuading. In past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some of your pupils may have missed opportunities to disclose such abuse during the lockdowns or periods of absence. Please view the DFE document online safety to view harms and their meanings.

https://outlook.office.com/mail/deeplink?AttachmentId=AQMkADA2OGFmZTcwLWI3NGMtNGRhZC1hYjNlLTdkZmI0NjA0NzFlZABGAAADJ%2FCCnDCB6EuT6kTN9W8GOgcAt8mCA99SvkSFSyjM%2BgEbIgAAAgEMAAAAt8mCA99SvkSFSyjM%2BgEbIgABX54iQgAAAAESABAAEgQBOQKzyEq0FzXgjw2v1g%3D%3D&ItemId=AQMkADA2OGFmZTcwLWI3NGMtNGRhZC1hYjNlLTdkZmI0NjA0NzFlZABGAAADJ%2FCCnDCB6EuT6kTN9W8GOgcAt8mCA99SvkSFSyjM%2BgEbIgAAAgEMAAAAt8mCA99SvkSFSyjM%2BgEbIgABX54iQgAAAA%3D%3D&AttachmentName=Teaching_online_safety_in_school.pdf

Computing Lead – Leanne Piano
Key responsibilities:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum

Subject leaders
Key responsibilities:

- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL (Designated Safeguarding Lead) /OSL(Online Safeguarding Lead) and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Teaching and Learning

Why use of the Internet is important?

- The Internet is an essential element in 21st century life in education, business and social interaction. The Academy has a duty of care to all pupils to provide quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The Academy internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children.
- Pupils will be taught what internet use is appropriate and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Development

This e-safety policy has been developed by a working group / committee made up of:

- Headteacher: Mrs A Brett
- SLT: Mrs A Brett and Mr S Ratcliffe
- E-Safety Officer: Mrs E Sanger
- Board of Directors

Consultation with the whole Academy community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Board of Directors*	October 2021
The implementation of this e-safety policy will be monitored by the:	*Headteachers, SLT, E-Safety Officer and the Board of Directors.*
Monitoring will take place at regular intervals:	*Annually*
The *Board of Directors* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually October 2021*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new	*Review Date: September 2022*

threats to e-safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Safeguarding Officer, Police, SLT and e-safety officer*

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)

Scope of the Policy

This policy applies to all members of the Academy, volunteers, parents, visitors, who have access to and are users of Academy ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers the Headteacher to regulate the behaviour of students when they are off the Academy 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 Academy, but is linked to membership of the Academy.

The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of Academy.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the Academy.

Board of Directors

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about e-safety incidents and monitoring reports. The Directors have an E-Safety Director.

The role of the E-Safety Director will include:

- Meetings with the E-Safety Officer
- Monitoring of e-safety incident logs
- Monitoring of filtering
- Reporting to relevant committee meeting
- Attending relevant E-Safety training

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the Academy community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Officer.
- The Headteacher and SLT are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety Officer

- Will support staff in providing termly current e-safety lessons throughout the school to raise awareness
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy e-safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff in following the SMART rules
- Liaises with the relevant body
- Liaises with Academy's technical support team IDT
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Meets regularly with E-Safety Director to discuss current issues, review incident logs and filtering
- Sanctions will be the responsibility of the Headteacher, SLT and the e-safety officer

Network Provider IDT

Key Responsibilities

- **T**hat the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- That the Academy meets required e-safety technical requirements
- That users only access the networks and devices through a properly enforced password protection
- The filtering system by the service provider is updated regularly
- That the use of the internet/email is regularly monitored in order that any misuse can be reported to the Headteacher, SLT and E-Safety Officer for investigation

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out by the e-safety officer
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy e-safety policy and Acceptable Use Agreements)
- The E-Safety Officer will receive regular updates through attendance at external training events. E.g., Online safety live via UK Safer Internet Centre
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training to individuals as required.
- All staff will teach e-safety each term to their class pupils
- All staff will get involved each year in the Internet Safety Day

Teaching and Support Staff

Key responsibilities

In 2021 pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies.

- Recognise that RSHE is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (Know what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the schools Safeguarding policy
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – report to the DSL lead.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

- They have an up-to-date awareness of e-safety current practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher, SLT and E-Safety Officer for investigation
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official Academy systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- All staff will take steps to prevent cyber-bullying.
- All staff monitor that pupils adhere to and follow the e-safety and acceptable use policies
- All staff monitor that the SMART rules are being adhered to
- All staff monitor that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- All staff where internet use is pre-planned for lessons, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
-

Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Pupils

Key responsibilities

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems
- Are responsible for using the Academy digital technology systems in accordance with the Pupil Acceptable Use Policy
- All children must follow the SMART rules stay safe system
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- Should understand the importance of adopting good e-safety practice when using digital technologies out of Academy and realise that the Academy's E-Safety Policy covers their actions out of Academy, if related to their membership of the Academy

Education – parents / carers

The Academy will raise parents and carers awareness of e-safety; the need to teach their children responsible use of the Internet and monitor what sites their children are using in order to ensure that they only access age-appropriate social media.

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Parents evenings, e-safety evenings
- High profile event e.g., Safer Internet Day

Parents / Carers

Key responsibilities

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school and school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The Academy will take every opportunity to help parents understand these issues through parents' e-safety evenings, newsletters, letters, website literature. Parents and carers will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:
- Digital and video images taken at Academy events
- Access to parents' sections of the website
- Their children's personal devices in the Academy (where this is allowed)

Parent Fact Sheets and Guides to Popular Social Media.
Click on the following links to find some useful guides to the following social media sites.

Fortnite https://www.youtube.com/c/fortnite

Put these below into your browser for latest information
YouTube
Tik Tok (formally Musically)
Instagram
Snapchat

Jessie and Friends https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/
To see the latest information for parents on how to keep their 4–7-year old's safe on line,

https://www.digismart.net/esafety.html

Internet Safety Resources
There is a great new online safety tools designed for parents launched by the Department for Education called **Parent Info**. It has advice on everything from keeping children safe from online trolls to WhatsApp - a guide for parents.

Use of digital and video images

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Staff can take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. These images should only be taken on Academy equipment only and the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the Academy website or media outlets

Data Protection

The Data Protection Policy 2021 has been updated with new amendments, see link below for information on data protection

https://cpdonline.co.uk/knowledge-base/business/data-protection-in-schools-all-you-need-to-know/

- Always take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in protected devices when they are using personal data.
- Transfer data using encryption and secure password

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted, or password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete

GDPR

- It is important that governing bodies and proprietors are aware that among other
- obligations, the Data Protection Act 2018 and the GDPR place duties on organisations
- and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Academy currently considers the benefit of using these technologies for education outweighs their risks. When using communication technologies, the Academy considers the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Leadership team/e-safety officer – in accordance with the Academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff, pupils or parents' email, chat, must be professional in tone and content. These communications may only take place on official Academy systems.
- EYFS/KS1/2 email addresses will be provided with individual Academy email addresses for educational use.
- Any staff member communicating with pupils must use Academy email and must always copy in the Leadership team.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details.
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff.

Online Safety

As schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate

monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online is provided in Annex C.

Cyber Bullying for staff **See link below**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Cyber Bullying for parents/carers **See link below**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf

Sexting **See link below**

https://www.thinkuknow.co.uk/professionals/guidance/sexting-guidance-wales/

https://www.gov.uk/government/organisations/uk-council-for-internet-safety

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835733/Keeping_children_safe_in_education_2019.pdf Annex C Page 96

Social Media - Protecting Professional Identity
Expectations for teachers' professional conduct are set out in 'Teachers Standards 2015'. Ofsted's e-safety framework updated 2016 reviews how online safety is now included in Ofsted's safeguarding documentation. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education pdf Annex C page 62

All Academies have a duty of care to provide a safe learning environment for pupils and staff. Academies could be held responsible, indirectly for acts of their employees during their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Academy through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

Academy staff should ensure that:
- No reference should be made in social media to pupils, parents / carers or Academy staff
- They do not engage in online discussion on personal matters relating to members of the Academy community

Online Sexual abuse:
A record number of reports of online child sexual abuse have been processed by the UK's Internet Watch Foundation that the availability of illegal content online is increasing.
The Internet Watch Foundation (IWF), a partner in the UK Safer Internet Centre and the UK charity responsible for finding and removing images and videos of child sexual abuse from the internet, processed more than a quarter of a million reports in 2019. It is our duty as a school to ensure that we keep all safe ensuring firewall systems are up to date. See link below for more resource information.
https://www.saferinternet.org.uk/blog/

Parents/Carers
Updated information on the link below about keeping your child safe online
https://www.nspcc.org.uk/keeping-children-safe/online-safety/?

Protecting children from the risk of radicalisation **(PREVENT)**
Is part of schools' wider safeguarding duties and is similar in nature to protecting children from other harms (e.g., drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. The school is aware of the increased risk of online radicalisation, as terrorist

organisations such as ISIL seek to radicalise young people using social media and the internet. This is managed as part of this e-safety policy, linked with the safeguarding policy and the ICT policy.

Unsuitable / inappropriate activities

The Academy believes that pupils and staff must not engage in unsuitable or inappropriate activities in an Academy context and that users should not engage in these activities in Academy or outside Academy when using Academy equipment or systems.

Responding to incidents of misuse

If a pupil suspects unsuitable or inappropriate activities are taking place, they must inform their class teacher/staff. If a member of staff suspects unsuitable or inappropriate activities are taking place, they must inform the Leadership team immediately. This guidance is intended for staff to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the Leadership team must be informed so that the police and CEOP can be informed appropriately.

Other Incidents

All members of the Academy community will be responsible users of digital technologies, who understand and follow Academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the Academy 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 Academy 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 as follows:

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within Academy and outside Academy. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access always.

The Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
  The Academy will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users

Policies to view:

Staff Acceptable users' policy 2021
Parents' Acceptable users' policy 2021
Pupils' Acceptable users' policy 2021
ICT Policies action plan 2021

Date: 08/9/21 To be reviewed by September 2022

Chair of Directors Signature: P Hurd