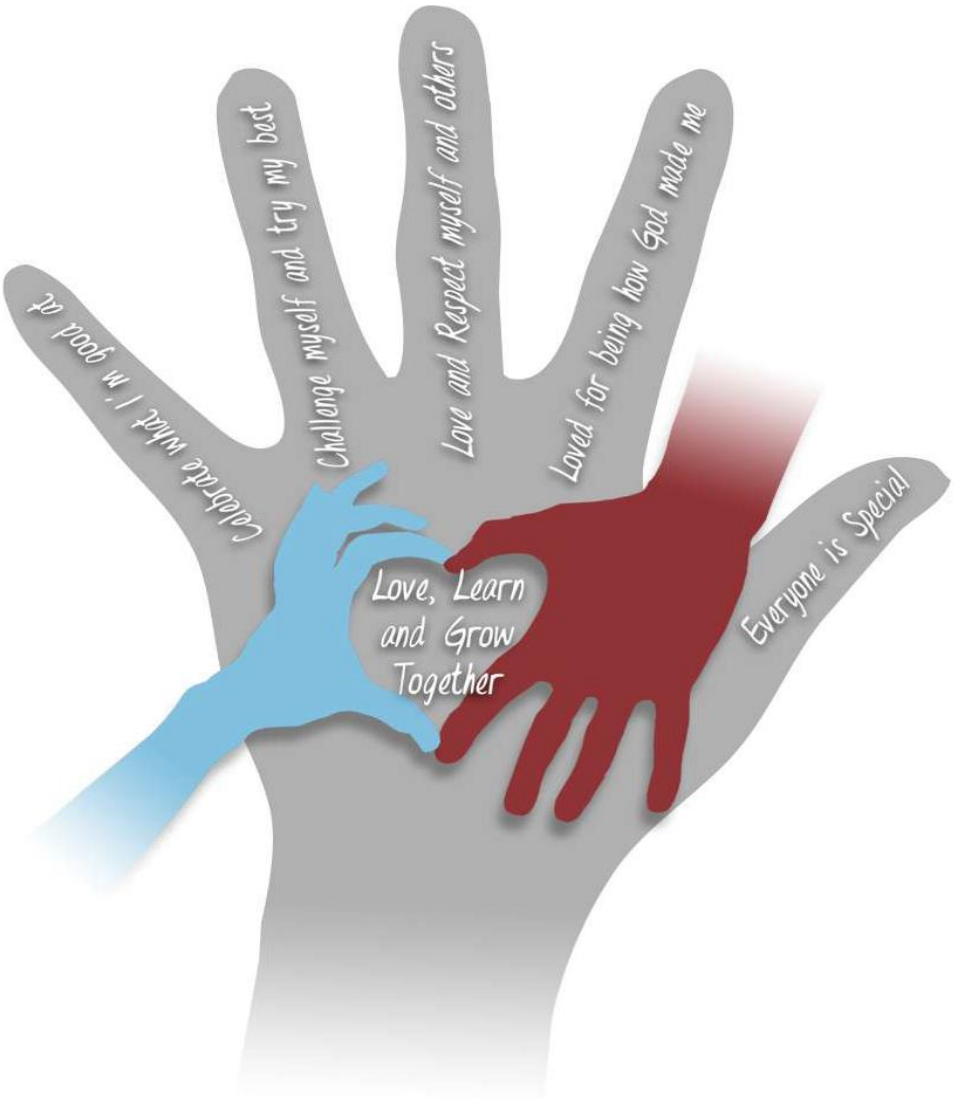
SJF **POLICY**

Online Safety

ST CLARE
Catholic Multi Academy Trust

DETERMINATION HONESTY RESPECT PASSION TEAMWORK SELF BELIEF

Love, Learn and Grow Together



OUR MISSION &VISION

Our vision is that every single member of our community will love, learn and grow together. This is achieved by:

- **Celebrating** what we are good at
- **Challenging** ourselves and doing our very best in our work
- **Loving** and **respecting** ourselves and each other
- **Knowing** that we are loved for being just how God made us
- **Accepting** that everyone is special

Introduction

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' 2023 (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 our school's statutory Safeguarding Policy.

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, antisemitism, radicalisation and extremism
- 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

Our school aims to:

- Set out expectations for all St John Fisher's Catholic Academy community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- 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 today's 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
    - for 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

Scope of the Policy

This policy applies to all members of St John Fisher School and community, (including staff, supply staff, Local Academy Committee Members, students / pupils, volunteers, parents/ carers, work placement students, visitors and community users) who have access to and are users of our digital technology, networks and systems, whether onsite or remotely, or use technology in their school role.

This policy is based on the Department for Education's (DfE's) 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 head teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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.

Schedule for Development Monitoring and Review

Title	**St John Fisher Primary – A Voluntary Catholic Academy Online safeguarding Policy**
Version	*2.0*
Date	*31-01-2024*
Author	*Mrs MM Barrett*
Approved by the Governing Body on:	
Monitoring will take place at regular intervals:	*Yearly basis with some sections reviewed ½ yearly*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any Online safeguarding incidents at regular intervals:	*At least once a year*
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online safeguarding or incidents that have taken place. The next anticipated review date will be:	*31.01.2025*
Should serious Online safeguarding incidents take place, the following external persons / agencies should be informed:	

St John Fisher will monitor the impact of the policy using:

- Logs of reported incidents
- External monitoring data for network activity
- Surveys/questionnaires of
    - Students/pupils (including every child matters Survey where applicable)
    - Parents/Carers
    - Staff

Communication of the Policy

- The senior leadership team will be responsible for ensuring the school community are aware of the existence and contents of the school's online safeguarding policy and the use of any new technology as and when appropriate.
- The online safeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and appropriately communicated to all members of the school community.
- Any amendments will be discussed by the School Student Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An online safeguarding training programme will be established across the school and will include a regular review of the online safeguarding policy.
- Online safeguarding training will be part of the induction programme / transition programme across the Key Stages.
- The school approach to online safeguarding and its policy will be reinforced through the curriculum.
- The key messages contained within the online safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed Online safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The Online safeguarding policy will be introduced to the students at the start of each academic year.
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

We believe that online safeguarding is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities technology offers in learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Local Academy Committee Members:

Local Academy Committee Members (LACM) are responsible for the approval of the online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *LACM* receiving regular information about online safety incidents and monitoring reports. A member of the *Local Academy Committee Members Body* has taken on the role of *online safety lead* (The Child Protection / Safeguarding Member)

- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- "Ensure appropriate filters and appropriate monitoring systems are in place being careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum.

The role of the online safety member will include:

- regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Support the school in encouraging parents and the wider community to become engaged in online safety activities

Responsibilities of Headteacher and Senior Leaders- Frank Barratt

The Headteacher has overall responsibility for safeguarding all members of the school community, though the day to day responsibility for online safeguarding will be delegated to the Online Safety Co-ordinator.

- The Headteacher and senior leadership team are responsible for ensuring that the Online safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their Online safeguarding roles and to train other colleagues when necessary.
- The Headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal Online safeguarding role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the Online safety Co-ordinator.
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious Online safeguarding incident. (see flow chart on dealing with Online safety incidents included in a later section) and relevant Local Authority HR / disciplinary procedures.
- The Headteacher and senior leadership team receive update reports of any incidents from the Online safeguarding/Safeguarding team.

Responsibilities of the Online safety Lead/Deputy Safeguarding Lead:- Mags Barrett

- To ensure that the school's online safeguarding policy is current and relevant; creating and maintaining Online safeguarding policies and procedures.
- To ensure that the school's online safeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school's Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.
- To promote an awareness and commitment to Online safeguarding throughout the school.
- To be the first point of contact in school on all Online safeguarding matters.
- To take day-to-day responsibility for Online safeguarding within school and to have a leading role in establishing and reviewing the school Online safeguarding policies and procedures.
- To lead the school Online safeguarding group or committee.
- To communicate regularly with school technical staff.
- To communicate regularly with the designated Online safeguarding Local Academy Member.
- To communicate regularly with the senior leadership team.
- To develop an understanding of current Online safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online safeguarding issues.
- To ensure that Online safeguarding education is embedded across the curriculum.
- To ensure that Online safeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online safeguarding issues to the Online safeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online safeguarding incident.
- To ensure that an Online safeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- 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 – never think that someone else will pick it up
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections). Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- Read and follow this policy in conjunction with the school's main safeguarding policy
- To understand, contribute to and promote the school's Online safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the Online safeguarding coordinator.
- To develop and maintain an awareness of current Online safeguarding issues and guidance including online exploitation, radicalisation and extremism, bullying, sexting etc.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.

- To embed Online safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of Online safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using only approved and encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To understand, contribute to and help promote the school's Online safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any Online safeguarding related issues that come to your attention to the Online safeguarding coordinator.
- To develop and maintain an awareness of current Online safeguarding issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the senior management team, local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, Local Academy Committee Members, work placement students and volunteers

Communication between adults and between children, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, Local Academy Committee Members and volunteers should:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.

- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child or parent/carers on social networks.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children, parent/carers so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children and young people in their care or parents/carers (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the school into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Designated Safeguarding Lead

- To understand the issues surrounding the sharing of personal or sensitive information and to ensure that personal data is protected in accordance with the Data Protection Act 1998.
- To understand the risks and dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving the grooming of children and young people in relation to sexual exploitation, radicalisation and extremism.
- To be aware of and understand online bullying and the use of social media and online gaming for this purpose.

Responsibilities of Students

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of Online safeguarding policies and practices and to adhere to those the school creates.
- To know and understand school policies on the use of digital technologies including mobile phones, digital cameras and any other personal devices.
- To know and understand school policies on the use of mobile phones in school.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the potential risks such as online exploitation, radicalisation, sexting and online bullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss Online safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting Online safeguarding.
- To read, understand and promote the school's Online safeguarding policy and the pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online safeguarding concerns with their children, be aware of what content, websites and Apps they are using, apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology and social media.
- To consult with the school if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

To sign a home-school agreement containing the following statements

- *We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community*
- *We will support the school's Online safeguarding Policy.*
- *Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet*
- *Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.*
- *Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school*
- *Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.*

Responsibilities of Other Community/ External Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

- Any external users/organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision, filtering and monitoring exist when external users/organisations make use of the internet and ICT equipment within school.

Education

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a safe and responsible approach. The education of students in Online safety is therefore an essential part of the school's Online safety provision. Children and young people need the help and support to recognise and mitigate risks and build their resilience online.

Online safety will be part of a broad and balanced curriculum and staff will reinforce Online safety messages. The Online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned Online safety curriculum will be provided as part of Computing / PHSE / SRE and other lessons and should be regularly revisited.
- Key Online safety messages will be reinforced as part of a planned programme of assemblies, including promoting Safer Internet Day each year.
- Students will be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- We will discuss, remind or raise relevant Online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- In lessons where internet use is pre-planned, it is best practice that students 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
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- All use will be monitored and they will be reminded of what to do if they come across unsuitable content.
- Students will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Students will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies; e.g. mother/father or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

All Staff (including Governors)

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

- All staff will receive regular information and Online safeguarding training through a planned programme of staff meetings every term.
- All new staff will receive Online safety information and guidance as part of the induction process, ensuring that they fully understand the Online safeguarding policy and Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the Online safeguarding of children and know what to do in the event of misuse of technology by any member of the school community.
- This Online safeguarding policy and its updates will be presented to and discussed by staff in staff meetings.
- An audit of the Online safety training needs of all staff will be carried out regularly.
- The Online safety Coordinator will provide advice, guidance and training as required.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and responsible way and in promoting the positive use of the internet and social media. Many have only a limited understanding of Online safety risks and issues, yet it is essential they are involved in the Online safety education of their children and in the monitoring of the children's online behaviours. Parents may under-estimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters and the school website
- Parents / Carers sessions
- High profile events
- Reference to the relevant web sites / publications

Training – Local Academy Committee Members

Local Academy Committee Members should take part in Online safety training and awareness sessions, with particular importance for those who are members of any sub committees involved in technology / Online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Safeguarding Children Board / Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Education – The Wider Community

The school will provide opportunities for local community groups of the community to gain from the school's Online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and Online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide Online safety information for the wider community*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and students instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and their legal responsibilities and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff will inform and educate students about the risks and current law associated with the taking, sharing, use, publication and distribution of images. In particular they should recognise the risks attached to publishing inappropriate images on the internet or distributing through mobile technology.
- Staff are allowed to take digital / video images to support educational aims or promote celebrations and achievements, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment, including mobile phones, of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. Staff will be aware of those students where publication of their image may put them at risk.
- Students' full names will not be used in association with photographs.
- Written permission from parents or carers will be obtained at the beginning of each year before photographs of students are published on the school website.
- When searching for images, video or sound clips, students will be taught about copyright and acknowledging ownership.

Managing ICT systems and access: Technical infrastructure, equipment, filtering and monitoring

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible and meets recommended technical requirements.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested weekly.
- The infrastructure and appropriate hardware are protected by active, up to date virus software.
- There will be regular reviews and audits of the safety and security of technical systems.
- The ACS Group is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place All users will have clearly defined access rights to school / college technical systems and devices.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the Pupil Acceptable Use Policy. They will ensure they log out after each session.

- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the staff AUP at all times.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to Mags Barrett, as agreed.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

- An agreed policy is in place that allows staff to and also forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning both within and beyond the classroom. This has led to the exploration of users bringing their own devices in order to provide a greater freedom of choice and usability. However, there are a number of Online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments.

BYOD raises a number of data protection issues as the device belongs to the user and not the Data Controller. It is crucial that the School ensures that all processing of personal data under their control continues to comply with the Data Protection Act 1998.

The 7th Principle of the Act states 'appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data'.

Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use policies, auditing and monitoring. This list is not exhaustive and school should have a BYOD policy and reference made within other relevant policies.

It is important that everyone connecting their device to your system understands their responsibilities and regular checks should take place to ensure that the policy is being adhered to.

Key Points:

- Implement an Acceptable Use Policy for Staff and Pupils to provide guidance and specify accountability of behaviour. Include end users in the development of the AUPs.
- Ensure you have a Social Media Policy – BOYD may lead to an increase in use of social media.
- Have clear guidance regarding what type of personal data may or may not be processed on personal devices.

Guidance for BOYD:

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated. Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises

- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, damage or theft will be reported as stated in the incident management process.
- Any inappropriate content brought into school on a personally-owned device, will be deleted or the device will be confiscated through the incident management process and the appropriate staff in school informed. Where necessary this may involve escalation to the police/social services.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by ICT4Schools
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed, sent or received through the school's internet provision.
- The school will ensure that the filtering system will block extremist content and protect against radicalisation in compliance with the Prevent Duty, Counter-Terrorism and Security Act 2015
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online safety Lead. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online safety Lead.
- The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and Government Prevent block list and this will be kept updated..
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Key Stage 2 students will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems.
- All information systems require end users to change their password at first log on.
- Staff will be prompted to change their passwords at any time that they feel their password may have been compromised.
- Staff should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Data Protection

Personal Data

The school has access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children, members of staff, volunteers, parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families

The Data Protection Act 1998 requires every organisation processing personal data to notify with the Information Commissioner's Office, unless they are exempt.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (F.Barratt) is familiar with information risks and the organisation's response. They have the following responsibilities

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management

Information Asset Owner (IAO)

Organisations should also identify an IAO for each asset or group of assets within school. For example, the school's management information system should be identified as an asset and should have an IAO. The role of an IAO is to understand

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The School will:-

- At all times 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 which they are using personal data or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.

- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

For the transmission of sensitive information or personal data e.g. by email it must be transferred by a secure method so it is protected from unauthorised access.

Email

Sensitive information must not be included within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

Encryption makes a file non readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

Communication Technologies

	Staff & other adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones/cameras				X				X
Use of other mobile devices e.g. tables, gaming devices		X					X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails		X						X
Use of messaging Apps		X						X
Use of social media		X						X
Use of blogs	X							X

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any agreed channel of digital communication between staff and students or parents / carers must be professional in tone and content.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 Radicalisation or extremism in relation to the Counter Terrorism and Security Act 2015					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)					X	
On-line gambling					X	

On-line shopping / commerce (educational)	X				
On-line shopping / commerce (non educational)				X	
File sharing (educational)	X				
File sharing (non educational)				X	
Use of social media (educational)	X				
Use of social media (non educational)				X	
Use of messaging apps (educational)			X		
Use of messaging apps (non educational)				X	
Use of video broadcasting eg Youtube (educational)	X				
Use of video broadcasting eg Youtube (non educational)				X	

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material, radicalisation and extremism
- other criminal conduct, activity or materials

The SSCB flow chart should be consulted and actions followed in line with the flow chart.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

It is intended that incidents of misuse will be dealt with through normal disciplinary procedures as follows:

Students Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Senior Leadership Team	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X		X
Unauthorised use of non-educational sites during lessons	X							X	X
Unauthorised use of mobile phone / digital camera / other handheld device	X	X				X		X	X
Unauthorised use of social networking / instant messaging / personal email	X	X						X	X
Unauthorised downloading or uploading of files	X	X						X	X
Allowing others to access school network by sharing username and passwords	X					X		X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X			X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X							X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X	X		X		X	X
Continued infringements of the above, following previous warnings or sanctions		X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X	X	X	X			
Using proxy sites or other means to subvert the school's filtering system					X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			X	
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X			

Staff

Actions / Sanctions

Incidents:	Refer to Senior leadership team	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X		X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X				X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X				X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X				X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X		
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X		X
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Dealing with Online Complaints

The nature of the internet, and the two-way communication that it brings, means that some parents will now turn to the online world to air their concerns or grievances. This may be through comments on the school twitter or facebook account. Seemingly minor incidents can escalate quite quickly with Facebook pages or Whatsapp groups being formed where parents can discuss issues and gather support.

Management of our school digital footprint is as crucial as managing a personal one.

Key Steps

1. Ensure that all staff and governors are aware of how to report and react to negative online statements
2. Review your Acceptable Use Policies to ensure that they clearly state that staff and governors must not be drawn in to any online discussions.
3. Review and update your complaints procedure to include reference to not utilise online channels for complaints.

- Parents/Carers are reminded through the Home-School Agreement of appropriate complaints channels and procedures.
- The complaint policy/procedure is clearly detailed on the school website and within the Complaints policy
- All staff and governors are aware of how to report any negative online comments about the school or members of the school community.
- Staff and governors must under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the Headteacher.