ST MARGARET'S CHURCH OF ENGLAND ACADEMY

Diocese of Liverpool

Principal
Mr S Brierley

"Achievement by faith and work"

(School Mission Statement)

POLICY ON: E13 Online Safety

Rationale

This Online-Safety Policy has been written by the school, building on Statutory Safeguarding Guidance (Keeping children safe in education) from the DFE. It has been agreed by the Senior Leadership team and approved by Governors. It is reviewed annually but by nature is a fluid document because of the context of the "Digital World".

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements
Persons responsible for this policy and to whom observations and comments should be made:

Mr. S Slater	Vice Principal
Mr D Silverstone	Assistant Principal
Mrs. C Roberts	Coordinator of Marketing and E-Learning
Mr. P Oliver	Chair of Governors

Copies of this policy are available on the website and by request to: Governors, Staff and Parents.

Reviewed and updated: March 2018
Next review: March 2019

Approved by the Standing Committee on:

Mission and Values

Mission

Our Academy Mission Statement:

Inspired by the knowledge and love of God,
we all come together to learn
in a Christian community where we are valued
for who we are and who we could become.

Values

As an Academy we have adopted 8 Christian values which we feel are the basis of our community.

- A Christian community is a community of faith, and at the heart of faith is **TRUST**. Trust is about letting go – putting ourselves in God's, and in other people's, hands. Jesus told his followers to "*trust in God; trust also in me*"; so as we work together, we expect members of our community to be trustworthy and reliable, and not to let others down.
- Education is not just about academic learning; it is about personal development too. As we work together, we expect that good working relationships, and **FRIENDSHIP**s, will develop, between students as well as between members of staff. In John 15, Jesus explicitly calls his disciples not servants, but friends. As a community, we celebrate the selflessness of friendship.
- **JUSTICE** is another value that is central to our community. Justice is about appreciating that our well-being is inextricably linked to everyone else's. It is not just about our response when someone acts inappropriately; it is also about ensuring that everyone is accorded the dignity and the respect and that is rightfully theirs. Isaiah encouraged us to "*seek justice!*" – and we do.
- From time to time, however, we all get things wrong. Jesus commanded us to show **FORGIVENESS** to each other, and as a Christian community we seek to obey Him. Someone in the wrong should show self-discipline and apologise, making reparation where appropriate; someone who is wronged should accept an apology and not seek to humiliate.
- Education is about far more than chemicals, conjunctions and crotchets! As a community, we seek to foster **WISDOM** and true insight into the way life works – an understanding of the consequences of our thoughts, words and actions and an awareness of the true value of things. Such wisdom is rooted in a proper reverence for God: as the Psalmist puts it, "*the fear of the LORD is the beginning of wisdom*".
- St Paul looked back on his life and was able to say that he had "*run the race*" right to the end. All those involved in education need to demonstrate similar levels of **ENDURANCE** – learning is the ultimate life-long task, a marathon not a sprint. By showing patience and resilience we will ensure that no-one is left behind, and that all are able to achieve their God-given potential.
- These values will be all the easier for us if we show **COMPASSION**. Compassion is more than just sympathy: like Jesus, we aim to put ourselves in other people's shoes, understand their point of view, then do something about it – and thus to grow in faith.
- Underpinning all of these, we seek to be a community at **PEACE**. St Paul describes God as the God of peace. We therefore seek to demonstrate harmony, stability and security within our Christian community, downplaying dissention and accentuating the positive.

Contents

SECTION A

Whole school approach to the safe use of ICT

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
• Content: being exposed to illegal, inappropriate or harmful material;
• Contact: being subjected to harmful online interaction with other users; and
• Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Keeping children safe in education
Statutory guidance for schools and colleges
September 2016

Creating a safe ICT learning environment includes three main elements at this school:

- **An effective range of technological tools;**
- **Policies and procedures, with clear roles and responsibilities**
- **A comprehensive E-Safety education programme for pupils, staff and parents.**

Online Safety (for the purposes of this document Online Safety/E-Safety are treated as the same) is seen as an essential aspect of strategic leadership in this school and the Principal, with the support of Governors, aims to embed safe practices into the culture of the school. The Principal ensures that the Policy is implemented and compliance with the policy monitored.

The Principal has overall responsibility for Online Safety and this cannot be delegated.

The responsibility for implementing online-safety within the wider safeguarding agenda has been designated to a member of the Senior Leadership Team –Assistant Principal –DS

Coordination of Online-Safety policy and learning has been designated to the E-learning coordinator- CR.

The school maintains a strategy for online-safety as a live “working” document which is under constant review as part of the process within which the school audits its online-safety measures. (See later)

The school has drawn up robust AUPs (Acceptable Use Policies) for staff/volunteers and students and these have been refined as appropriate for Year 7-11, 12 and 13 and staff/volunteers. (See later section). There is a requirement for parents and pupils to sign these for Year 7-11 and pupils in Year 12 and 13 to sign.

The school includes online-safety in the curriculum for Computing and ICT and Learning for Life (PHSE) and ensures that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

Our IT support is provided by Convene IT who manage our network. We also have tow onsite technicians who administer many of the day to day network procedures.

The school uses an accredited supplier for internet services- this was until recently, LDL via the Local Authority and we now have a contract with a highly reputable Internet Service Provider, Spitfire with the infrastructure provided by BT.

Network and internet use is closely monitored and individual usage can be traced using auditing software tools by our onsite technicians and network services provider, Convene IT. Regular ICT security audits are initiated.

All personal data is collected, stored and used according to the principles of the Data Protection Act and Freedom of Information Act.

Internet access is provided by an approved educational internet service provider, Spitfire, which complies with DFE requirements.

Staff with responsibility for managing filtering, network access and monitoring are adequately supervised by a member of SLT (SS)

The school has responsibility for the content filtering and the two policies for users are robust and have been set up to reflect educational objectives and have been approved by SLT.

The school includes online safety measures in sections of its SEF and DSEF documents as appropriate. Improvements to the strategic use of ICT feature in the Academy Improvement Plan when appropriate.

Signage relating to acceptable use is prominent in all areas of the school including teaching, learning and administration areas and digitally on the intranet and website

Cyberbullying will be dealt with appropriately in line with school Anti Bullying Policy.

The school will keep appropriate records of incidents within the procedures of the behavior system.

Online safety information is available to stakeholders via our website.

The school will engage with parents over online-safety matters, and ensure that parents/guardians/carers have signed and returned the e-safety/AUP form appropriate to their child (ren)

Staff

The school recognises that it is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with the appropriate manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration and support, governors and helpers will be included in appropriate awareness raising and training.

Induction of new staff will include a discussion of the school's online safety policy

Regular training is provided through the staff CPD Programme.

Measures are in place in order for all staff to:

Understand online-safety issues and risks and have a good knowledge of appropriate procedures for

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social media;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- Cyberbullying procedures;
- their role in providing Online-Safety education for pupils;

Commented [cr1]: New para last year not included??

Receive regular training and awareness updates at Head of Department meetings, Head of Year meetings and whole school staff meetings/regular CPD. Updates are also issued as briefing notices and in bulletins published on paper and electronically by the E-learning coordinator.

Know how to respond to incidents involving breaches of online-safety and how to escalate an incident of concern.

Know the measures to take to ensure that data is kept safe and secure.

Know how to protect themselves online and how to conduct themselves professionally online, particular with the increasing prevalence of social networking sites - Staff should be aware that Internet traffic is monitored and can be traced to the individual user.

Learners

Understand what safe and responsible online behaviour means.

Receive online-safety education at appropriate places across the curriculum in Computing and ICT lessons and Learning for Life (PHSE).

Get the opportunity to improve their digital literacy skills

Are aware of the school's online-safety procedures through the distribution and signature of an Acceptable Use Policy (AUP), appropriate to their key stage and through prominent signage throughout the school buildings.

Must know how to report any concerns they may have.

Parents and governors

Essentially these stakeholders are:

- To be kept aware of e-safety issues and risks
- To understand their roles and responsibilities
- To receive regular training and updates

Internet use in pupils' homes is commonplace. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school should be able to help parents plan appropriate supervised use of the Internet at home.

Internet issues will be handled sensitively, and parents will be advised accordingly.

A partnership approach with parents is encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents via the school website

Parents' attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the School Website.

Internet issues will be handled with sensitivity to inform parents without undue alarm.

Links to relevant information from organisations such as SWGFL, UKSAFER INTERNET, BECTA, PIN, CEOP and NCH Action for children are available on the Website

For all aspects of children's e-safety parents can visit; www.thinkyouknow.co.uk. A link is provided on the school website.

A link is provided to the excellent materials provided on Digital Parenting.

Regular online safety hints and tips are distributed to stakeholders subscribing to the schools twitter feed.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on online-safety and are updated at least annually on policy developments.

SECTION B

Managing the Internet safely

Internet access – Overview of why this is important.

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Access to learning platforms and Virtual Learning Environments by staff, pupils and parents.
- Access to cloud computing services and resources.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- secure data exchange between local and government bodies.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime, radicalisation, extremism and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse. Risks can be high outside school, so this school is making information available to parents and carers.

The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Through our AUPs we are making it clear to users that the use of school equipment to view or transmit inappropriate material is "un-authorised" and infringements will be dealt with; and are ensuring that all reasonable and appropriate steps have been taken to protect pupils.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or by any consequences of Internet access. This is made clear in the Acceptable Use Policies.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

The Principal will ensure that the online-safety policy is implemented and compliance with the policy monitored.

Technical and Infrastructure Statements –

The school ICT systems will be reviewed regularly with regard to security and:-

Virus protection will be installed and updated regularly.

Security strategies will be regularly discussed with the appropriate external providers (Convene IT for our server hosting and Spitfire/BT?)

The school has responsibility for the content filtering and the two access policies for users are robust and have been set up to reflect educational objectives and have been approved by SLT;

Any concerns about the system will be communicated to providers so that systems remain robust and protect students;

Additional user-level filtering via a classroom management system has been successfully implemented – this uses an application called Impero;

Network health is ensured through appropriate anti-virus software and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;

The network administrators will remain up-to-date with appropriate services and policies;

The network administrators will check to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;

We will never allows pupils access to Internet logs;

Network auditing software is installed;

Use security time-outs on Internet access where practicable or useful;

Uses individual log-ins for pupils and all other users;

Impero 'remote' management control tools are used for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;

Never send personal data over the Internet unless it is encrypted or otherwise secured;

Never allow personal level data off-site unless it is on an encrypted device;

Encourage the use of 'safer' search engines with pupils such as activates 'safe' search where appropriate;

Ensures pupils only publish within appropriately secure learning environments

Internet policy and procedures

Context

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear.

In this school supervision is the key strategy. Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation. The following questions must be contemplated. Is it sufficient for a teacher or a learning support assistant to be in the area? Should Internet machines be placed in a common area between classrooms? Are there circumstances outside normal lesson time where pupils justifiably need access to the Internet?

Surfing the Web

Aimless surfing should never be allowed in school. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Pupils should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils broadly 'searching the Internet'.

Often a small selection of websites will be enough; the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites are a useful way to present this choice to pupils.

Teachers' web site selections for various topics can be put onto the learning or interest spaces on the network/cloud so pupils can, access out of school, from home etc.

Other links may be put on the school web site, although there may even be difficulties here. We need to remember that hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing, for example, to a pornographic one. Therefore, sites should always be previewed and checked.

Search Engines

Some common Internet search options are deemed as high risk, for example Google image search. The access policies have been set up to reflect content that may be deemed unacceptable for certain users
[NB: Images usually have copyright attached to them.]

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. The use of social networking software has become commonplace. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcasting (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web).

Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. However, schools should focus on using social collaboration tools within the learning platform and official school accounts such as @smaliverpool, @smasixth. The school deliberately does not have an official Facebook Page (see section on Social Media and the robust measures needed to manage accounts)

Internet Policy Statements

This school:

Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas, the internet lounge and study centre where older pupils have more flexible access;

We use a suitable filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature etc.; A flagging system is

incorporated within this software to indicate suitability. This indicates that sites are not accessible.

The school Internet access is designed specifically for pupils use and includes filtering appropriate to the age of pupils.

We have capacity for additional user-level filtering through Impero, so adapt filtering to the age of the pupils;

Staff should preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;

Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use as part of the ICT and Learning for Life curriculum.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of the pupils.

Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

Pupils will be educated in the effective use of Internet in research, including the skills of knowledge location and retrieval.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the supervising teacher who will report it to network manager.

The school should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;

Never allows / is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;

Informs users that Internet use is monitored;

Informs staff and students that that they must report any failure of the filtering systems directly to the network technicians via the designated service desk software. Our systems administrators report to LDL where necessary;

Blocks all Chat rooms and social networking sites with the exception of those that are part of an educational network or approved Learning Platform/online learning site; Pupils will not be allowed access to public or unregulated chat rooms.

Only uses approved systems for video conferencing activity;

Only uses approved or checked webcam sites;

Does not allow pupil access to music download or shopping sites; these are blocked by filtering software.

Requires pupils (and their parent/carer) at all Key Stages to individually sign an acceptable use agreement form which is fully explained and used as part of the teaching programme at the start of;

Uses school email, easy mail for email access in school by staff and pupils.

Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;

Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;

Keeps a record, e.g. print-out, of any bullying or inappropriate behavior for as long as is reasonable in-line with the school behavior management system;

Ensures the designated safeguarding officer has appropriate training;

Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the school;

Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;

Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA. (see Safeguarding Policy)

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The school will keep a record (signed AUP) of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.

How will the policy be introduced to pupils?

Rules for Internet access will be posted in and near all computer systems.
Pupils will be informed that Internet use will be monitored.
Teaching of effective and safe use of technologies in Computing and ICT lessons particularly in Year 7 but revisited in 8 and 9
Part of the core curriculum in Year 10
Participation in annual Safer Internet Day and assembly and follow up materials delivered.
Participation in Year 7 in "Our Community" programme.
Related activities may form part of retreat days
Use of outside providers to bolster support e.g. Brave the Rage, Bullybusters.
Instruction in responsible and safe use always precedes Internet access in year 7
A module on responsible Internet will be included in the Learning for Life programme covering both school and home use and.
A series of assemblies will be delivered annually on this and related matters by Assistant Principal RL.
Links to sites informing of good practice will be available on the website and displays on e-safety are visible around the building.
The school subscribes to Impero for classroom management and students experience the reality of its use in lessons.
The school subscribes to the SHARP system for reporting – a link to this is available on the website.
An Online Safety action plan is maintained each year. See appendix.

How will staff be consulted?

All staff must accept the terms of 'Responsible Internet Use' statement before using any internet resource in the school.

All staff, including teachers, supply staff, teaching assistants and learning support staff will have access to this School Online-Safety Policy, and its importance explained.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff development in safe and responsible Internet use and on school Internet policy will be provided as required and has featured in recent CPD.

All Staff are required to sign the staff AUP.
Staff Safeguarding Training and updates includes Online Safety (See appendix C of Sept 2016 DFE safeguarding guidance.
E-Learning Coordinator CR- attends regional briefings and cascades information back to stakeholders.

How will complaints regarding Internet use be handled?

Responsibility for handling incidents of student misuse is delegated to the pastoral team as per safeguarding requirements.
Any complaints about staff misuse must be referred to the Principal.

Pupils and parents will be informed of the complaints procedure.

Pupils and parents will need to work in partnership with staff to resolve issues.

Sanctions available are those appropriate through the SMART pastoral system and more severe measures as appropriate to the infringement committed.

SECTION C

Email Management

This school provides staff and students with a school email address (@stmargaretsacademy.com) through Office 365 which should be used for purposes of school work and business.

Pupils may only use approved e-mail accounts on the school system, and access in school to external/non-proprietary e-mail accounts may be blocked.

Pupils must immediately tell the supervising teacher if they receive an offensive e-mail who will then report it via the appropriate channel

Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.

Whole-class or group e-mail addresses may be used in all key stages.

E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school paper. See relevant clauses pertaining to this in staff and student AUPs.

The forwarding of chain letters is banned.

SECTION D

School Web Site

Although the website is hosted and managed by an external provider, the Principal and Marketing and E-Learning Coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate and compliant.

The point of contact on the web site is the school address, school e-mail and telephone number. Staff or pupils home information will not be published.

Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.

Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.

Written permission from parents or carers will be obtained before photographs of pupils will be published on the school Website. (Within the published policy for Images and permissions -obtained when the child joins the school)

The school Web site will comply with DFE guidelines for publications. It will be reviewed regular to ensure compliance.

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

SECTION E

Use of Digital and Video Images

This is carefully managed in school and all parents receive a letter and sign a permission form when their child starts at the school. The current version of this can be found in appendix. The use of these is covered by a separate school policy.

SECTION F

Use of Mobile Technologies

This is clearly documented in the school pastoral handbook – printed an online versions and the student information is contained in the annual student planner issued to each student in the school at the start of each academic year.

Essentially the use of mobile technology limited on school premises and all devices should be switched off, at all times, in lessons.
The school now has Wi-Fi connectivity. All traffic is routed through the same filtering systems as wired network communication.

Students in Years 7 to 11 are not permitted to use their own devices in school.

Sixth form students are issued with policy guidance regarding the use of Wi-Fi in the Sixth form communal areas.

Section G– Infringements Procedure

Responsibility for handling incidents of student misuse is delegated to the pastoral team in accordance with safeguarding requirements.

SECTION H

Social Media

Social media (e.g. Facebook, Twitter, LinkedIn, WhatsApp, SnapChat) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

St Margaret's CE Academy recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This section of the Online Safety policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy but it is advised that staff remain mindful of appropriate professional conduct.

Digital communications with pupils/students may also be considered. Staff may wish to use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control of Social Media

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation

- **Administrator / Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- **Process for creating new accounts**

  The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team and E Learning Coordinator which covers the following points:-
  - The aim of the account
  - The intended audience

- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
  - Engaging
  - Conversational
  - Informative
  - Friendly (on certain platforms, e.g. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.
  - **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
  - **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
  - Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
  - If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
  - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
  - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
  - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
  - The school permits reasonable and appropriate access to private social media sites where these are not blocked.

- **Pupil/Students**
  - **Staff are not permitted to follow or engage with current (or prior if u18) /students of the school on any personal social media network account.**
  - The school's education programme should enable the pupils/students to be safe and responsible users of social media.

- Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- **Parents/Carers**
  - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to the defined policy or process.

Summary of Guidance on Social Media

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don’ts

- Don’t make comments, post content or link to materials that will bring the school into disrepute
- Don’t publish confidential or commercially sensitive material
- Don’t breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
- Don’t post derogatory, defamatory, offensive, harassing or discriminatory content
- Don’t use social media to air internal grievances

St Margaret's Church of England Academy
Computer Network and Internet
Acceptable Use Policy – Sixth Form

The School's computer network is well established and plays a major role in the education of students at St Margaret's. In school, access to the internet is provided for the purpose of educational research and learning. We have developed this *Acceptable Use Policy* to provide rules and safeguards for the appropriate use of the internet.

In order to access work at home a device with a standard "high speed internet" connection is needed along with availability of programs within the Microsoft office suite, a printer would be a useful addition. The school recognises that not all students will have this equipment and has made provision for those students. Students who do not have this access at home should always make use of the Study Centre, Internet Lounge and subject department study support opportunities to complete work.

If you wish to gain access to the school computer network, email and internet and use the Wi-Fi connection when appropriate, then please read, sign and return the following agreement to the school. A copy of the signed agreement will be held on file by the school.

Student Agreement

I understand that access to the **school computer network and internet** from St Margaret's Academy must be in support of educational research or learning, and I agree to the following:

- I will refrain from accessing any newsgroups, links, list servers, web pages or other areas of cyberspace that would be considered pornographic, racist, violent, illegal or illicit.
- I will not use chat rooms or social networking sites unless as part of a teacher-led educational project.
- I am responsible for monitoring and appropriately rejecting materials, links, dialogues and information accessed, received by me.
- I will not use valuable internet time playing non-educational games.
- The school has effective web content filtering; I will not use any means to bypass the filtering system and search for inappropriate material.
- I will be courteous and use appropriate language. I will refrain from using obscene, harassing or abusive language and will report any cases of such usage against me to my teacher or the ICT department.
- I accept responsibility for compliance with copyright laws and will not allow copyrighted material to enter school. I will not download software, games, music, graphics, videos or text materials that are copyrighted or violate the law by distributing or posting these.
- Plagiarism is unacceptable. I will use downloaded material appropriately in assignments, listing its source in a bibliography and clearly identifying any quoted material.
- I will not reveal personal information, including names and addresses, bank details, telephones numbers of myself or others.
- I will not damage or tamper with any of the computer hardware, software or network equipment. Furthermore, if I discover any methods of causing such damage, I will report them to the ICT department and I will not demonstrate them to others.

- I will not attempt to change any computer, monitor or software settings on any school computers.
- I will abide by the current log-on procedures for access to the computer network. I will not disclose my password to anyone and I will not attempt to find out another person's password by any method, or to use that password to gain access to other peoples' work. If I suspect that my password is no longer secure, for example if someone else knows it I will report this to a member of staff so that it can be changed.
- I understand that the entire network is protected by anti-virus software and that students are advised to use anti-virus software on home computers and laptops.
- I will not attempt to obtain access any website restricted by the school or blocked by the filtering software
- I understand that work may be made available to me via online learning sites or "Cloud" based services and I will always endeavour to complete this work either at home or in school.
- I will not disclose any unique user name and password for online learning sites, e.g. Doddle, Show My Homework, and My Maths etc. to any other person.
- I will attempt to save my work correctly and use sensible file management techniques at all times.
- I will manage the space allocated to me for storing work and avoid storing multiple, identical copies of the same file or files that are not relevant to my school work
- I will use my allocation of printer credits carefully and only print work when necessary
- I will not take digital photographs, or edit digital images of staff or students without their consent.
- I will not bring in removable media from outside school, unless I have been given permission to do so. Memory sticks are prone to viruses and I understand that they must be used with care
- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, for example using the Wi-Fi connection, I must follow the rules set out in this agreement, in the same way as if I was using school equipment.

If I violate any of the terms of this agreement, I may be denied access to the Internet and/or computers for a time determined by the school and may face further disciplinary action as determined by the management of the school.

Student Email Policy

The purpose of this policy is to ensure the proper use of St.Margaret's email system and make users aware of what St.Margaret's deems as acceptable and unacceptable use of the email system. St.Margaret's reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any student disregards the rules set out in this Email Policy they may be fully personally liable.

Email is a business communication tool and students are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply.

The email account provided to you by St Margaret's CE Academy must only be used in support of educational research or learning, and in agreement with the following:

- You must not send emails with any libelous, defamatory, offensive, racist or obscene remarks.
- You should never forward emails with any libelous, defamatory, offensive, racist or obscene remarks.
- You must not unlawfully forward confidential information.
- You should not forward or copy messages without permission.
- If you send an attachment that contains a virus, you and St.Margaret's can be held liable.

The following rules are required by law and are to be strictly adhered to:

- **It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify a member of staff.**
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not disguise or attempt to disguise your identity when sending mail.

St.Margaret's considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image. Therefore St.Margaret's wishes student's to adhere to the following guidelines:

Writing emails:

- Write well-structured emails, composing short descriptive messages.
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending.
- Do not write emails in capitals.
- Only mark emails as important/urgent if they really are important/urgent.
- It is polite to check and reply to emails regularly

Maintenance:

- Delete any email messages that you do not need to have a copy of.

I will abide by the expectations set out in this contract when using any web-based email account in school.

If I violate any of the terms of this agreement, I may be denied access to an email account in school for a time determined by the school and may face further disciplinary action as determined by the management of the school.

Acceptable Use Agreement

(This form relates to the student Acceptable Use Agreement, to which it is attached)

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

- I understand that St. Margaret's CE Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

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

- I use the academy systems and devices (both in and out of school).
- I use my own devices in the academy (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the academy in a way that is related to my being a member of this academy e.g. communicating with other members of the school, accessing school email, VLE, websites etc.

Student to sign

Student Name (Print) ……..Form ……..

Signed …….
Date……..

St Margaret's CE Academy Computer Network and Internet Acceptable Use Policy

The School's computer network is well established and plays a major role in the education of students at St Margaret's CE Academy. In school, access to the internet is provided for the purpose of educational research and learning. We have developed this *Acceptable Use Policy* to provide rules and safeguards for the appropriate use of the internet.

In order to access work at home a device (laptop or PC) with a standard "high speed internet" connection is needed along with availability of programs within the Microsoft office suite, a printer would be a useful addition. The school recognises that not all students will have this equipment and has made provision for those students. Students who do not have this access at home should always make use of the Learning Resource Centre and ICT department study support opportunities to complete work.

If you wish your son to gain access to the school computer network and internet and use the Wi-Fi connection, when appropriate, then please read, sign and return the following agreement to the school (via form tutor). A copy of the signed agreement will be held on file by the school.

Student Agreement

I understand that access to the **school computer network and internet** from St Margaret's CE Academy must be in support of educational research or learning, and I agree to the following:

- I will refrain from accessing any newsgroups, links, list servers, web pages or other areas of cyberspace that would be considered pornographic, racist, violent, illegal or illicit.
- I will not use chat rooms or social networking sites unless as part of a teacher-led educational project.
- I am responsible for monitoring and appropriately rejecting materials, links, dialogues and information accessed, received by me.
- I will not use valuable internet time playing non-educational games.
- The school has effective web content filtering; I will not use any means to bypass the filtering system and search for inappropriate material.
- I will be courteous and use appropriate language. I will refrain from use of obscene, harassing or abusive language and will report any cases of such usage against me to my teacher or the ICT department.
- I accept responsibility for compliance with copyright laws and will not allow copyrighted material to enter school. I will not download software, games, music, graphics, videos or text materials that are copyrighted or violate the law by distributing or posting these.
- Plagiarism is unacceptable. I will use downloaded material appropriately in assignments, listing its source in a bibliography and clearly identifying any quoted material.
- I will not reveal personal information, including names and addresses, bank details, telephones numbers of myself or others.
- I will not damage or tamper with any of the computer hardware, software or network equipment. Furthermore, if I discover any methods of causing such damage, I will report them to the ICT department and I will not demonstrate them to others.

- I will not attempt to change any computer, monitor or software settings on any school computers.
- I will abide by the current log-on procedures for access to the computer network. I will not disclose my password to anyone and I will not attempt to find out another person's password by any method, or to use that password to gain access to other peoples' work. If I suspect that my password is no longer secure, for example if someone else knows it I will report this to a member of staff so that it can be changed.
- I understand that the entire network is protected by anti-virus software and that students are advised to use anti-virus software on home computers and laptops.
- I will not attempt to obtain access to any website restricted by the school or filtering software
- I understand that work may be made available to me via online learning sites and I will always endeavour to complete this work either at home or in school.
- I will not disclose any unique user name and password for online learning sites, e.g. Doddle, Show My Homework, and My Maths etc. to any other person.
- I will attempt to save my work correctly and use sensible file management techniques at all times.
- I will manage the space allocated to me for storing work and avoid storing multiple, identical copies of the same file or files that are not relevant to my school work
- I will use my allocation of printer credits carefully and only print work when necessary
- I will not take digital photographs, or edit digital images of staff or students without their consent.
- I will not bring in removable media from outside school, unless I have been given permission to do so. Memory sticks are prone to viruses and I understand that they must only be used by staff.
- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, for example using the Wi-Fi connection, I must follow the rules set out in this agreement, in the same way as if I was using school equipment.

If I violate any of the terms of this agreement, I may be denied access to the Internet and/or computers for a time determined by the school and may face further disciplinary action as determined by the management of the school.

St.Margaret's CE Academy Student Email Policy

The purpose of this policy is to ensure the proper use of St.Margaret's email system and make users aware of what St.Margaret's deems as acceptable and unacceptable use of the email system. St.Margaret's reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

By following the guidelines in this policy, the email user can minimise the legal risks involved in the use of e-mail. If any student disregards the rules set out in this Email Policy they may be fully personally liable.

Email is a business communication tool and students are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply.

The email account provided to you by St Margaret's CE Academy must only be used in support of educational research or learning, and in agreement with the following:

- You must not send emails with any libelous, defamatory, offensive, racist or obscene remarks.
- You should never forward emails with any libelous, defamatory, offensive, racist or obscene remarks.
- You must not unlawfully forward confidential information.
- You should not forward or copy messages without permission.
- If you send an attachment that contains a virus, you and St.Margaret's can be held liable.

The following rules are required by law and are to be strictly adhered to:

- **It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify a member of staff.**
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not disguise or attempt to disguise your identity when sending mail.

St.Margaret's considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image. Therefore St.Margaret's wishes students to adhere to the following guidelines:

Writing emails:

- Write well-structured emails, composing short descriptive messages.

- Use the spell checker before you send out an email.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending.
- Do not write emails in capitals.
- Only mark emails as important/urgent if they really are important/urgent.
- It is polite to check and reply to emails regularly

Maintenance:

- Delete any email messages that you do not need to have a copy of.

I will abide by the expectations set out in this contract when using any web-based email account in school.

If I violate any of the terms of this agreement, I may be denied access to an email account in school for a time determined by the school and may face further disciplinary action as determined by the management of the school.

School Computer Network and Internet
Acceptable Use Statement

Please sign the following statement if you wish to apply for access to the school computer network and Wi-Fi, email and the internet

Student to sign

Student Name (Print) …… Form …….

Signed …… Date…….

Parental Agreement

As the parent/carer of _____

- I acknowledge that I have read the agreement (s) on student use of computers, online learning sites, email system/Wi-Fi and the internet at St Margaret's CE Academy and I have discussed it with my son.
- I understand that access is designed for educational purposes.
- I recognise that while student use of the internet and computers is monitored through high quality content filtering methods both in school and via the LA portal, it may be impossible to continually monitor and restrict access to all controversial materials.
- I further acknowledge that, whilst questionable material exists on the internet, the user must actively seek it and therefore is ultimately responsible for bringing such materials into school.
- I therefore do not hold the Principal or staff of St Margaret's CE Academy responsible for any such materials my son may acquire from the internet.
- I accept responsibility for setting standards for my son to follow when selecting, sharing and exploring information and media.

Parent/Carer to sign below

Name (Print) ……..

Parent/Carer of ……Form…….

Signed …….. Date …….

AUP – staff (staff who joined Pre 2015)

Staff Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-safety coordinator: Ms. A. Penketh, Deputy Head, Student Support.

- I will only use the school's secure email / Internet / Intranet / Learning Portal and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Such personal data can only be taken out of school or accessed remotely with authorisation and via secure system.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the appropriate permission.
- I understand that all my use of the Internet and other related technologies may be monitored and logged and can be made available, on request, to the Headmaster, or person designated by him.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature …….…… Date ……

Full Name …….....(printed)

Job Title . . . . . .

AUP – Staff (Current)

Staff Acceptable Use Agreement / Code of Conduct

New technologies are integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their work.

The school will try to ensure that staff and volunteers will have appropriate access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

This Policy should be read in conjunction with the current school Online Safety Policy.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and promote and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE's etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (see Online Safety Policy)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. (See Use of Digital Images Policy) I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g on the school website) I will ensure it is not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat on social networking sites in school in accordance with the school's policies. (See Online Safety Policy)
- I will only communicate with pupils and parents /carers using official school systems and not personal email accounts. Any such communication will be professional in tone and manner. (See Online Safety Policy)
- I will not follow or engage with current pupils of the school on any personal social media network account.
- I will not follow or engage with prior pupils of the school, under the age of 18, on any personal social media account.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile communication and storage devices in school, I will follow the rules set out in this agreement, in the same way as if I was using equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (See Online Safety Policy)
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will ensure that my data is regularly backed up, in accordance with relevant school policies and that I do not use excessive storage but regularly manage files I have stored on the computer system
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without permission. (See Online Safety Policy)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy).
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened using the helpdesk if possible.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Useful Links:

Online safety and acceptable use policy guidance

http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates

http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates

https://360safe.org.uk/

IAG on mechanisms the school might have in place to support pupils, staff and parents facing online safety issues?

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526153/Keeping_children_safe_in_education_guidance_from_5_September_2016.pdf

https://www.gov.uk/government/publications/what-to-do-if-youre-worried-a-child-is-being-abused--2

https://www.thinkuknow.co.uk/Teachers/blog/Dates/2013/3/Sexting-in-schools-What-to-do-and-how-to-handle-it/

http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring

http://www.ceop.police.uk/

Info for staff to ensure appropriate online safety training that is relevant and regularly updated? There is plenty of training material and courses provided by:

https://www.thinkuknow.co.uk/teachers/training/paidtrainingDetails/

http://www.childnet.com/teachers-and-professionals

http://www.onlinesafetylive.com/

http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

Info for children and young people to build knowledge, skills and confidence when it comes to online safety?

http://www.thinkuknow.co.uk/

http://www.childnet.com/resources%20young-people/

http://www.saferinternet.org.uk/advice-and-resources/young-people

http://swgfl.org.uk/products-services/esafety/resources/Digital-Literacy

Info for Parents

http://parentzone.org.uk/

http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers

http://www.childnet.com/resources/supporting-young-people-online

http://www.vodafonedigitalparenting.co.uk/

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

https://www.net-aware.org.uk/

http://parentinfo.org/

https://www.thinkuknow.co.uk/parents/

Online Safety Action Plan 2018-19

What	Already in Place	Action Required	Person(s) Responsible
Staff			
Understand online-safety issues and risks?	• Staff training and CPD • Info to staff issued recently – email or print • Info available on Staff : drive/E learning • Access to Online Safety Policy which contains guidance		**DS/CR** **CR** **CR** **CR**
Receive regular training and awareness updates?	• Staff CPD • Info to staff issued • Briefing bulletins • Staff Meetings • Website information		DS/CR
Know how to escalate an issue of concern?	• Clear procedure in place for breach of AUP. • Staff guidance issued as part of safeguarding procedures		DS/RK/VW
Know how to keep data safe and secure?	• Issued with unique user login/password for: Network, email PARS/SIMS etc.		Network Admin
Know how to protect themselves online?	• Staff training delivered • Information available in Staff :E learning • Safeguarding on agendas for meetings • Online Safety policy guidance		**DS/CR**
Know how to conduct themselves professionally online?	• Staff CPD • Staff meetings e.g. leadership/HODs/Hoys/Whole staff		**DS/CR**
Know about the online safety safeguarding guidance	• ITT trainees told, NQTs told • Regular staff CPD • E-Learning coordinator cascades messages from local briefings		**PK/DS/CR**

What	Already in Place	Action Required	Person responsible
Learners			
Understand what safe and responsible online behaviour means?	• Online-safety rules are displayed in all rooms where computers are used and expressed in a form that is accessible to all students? • Students accept AUP at first login • AUP issued at start of Year 7 and Post 16 and when new learners join		CR/Admin
Receive online-safety education at appropriate places across the curriculum?	• Computing Year 7 unit 7.1 Using Computers Safely and Effectively. Delivered in autumn term before they are allowed online • ICT Year 8,9,10 – Online safety refresher lessons at key points (See SOW) • ICT Year 12 and 13 - E safety refresher lesson. Delivered annually Autumn term • Regular feature of LFL – 7-11 • PHSE 12 and 13 • Work displays in ICT rooms • Safer Internet Day observed • Wellbeing/ASD/Dyslexia awareness and other special days may feature online safety messages for all or specific groups. • Assemblies/ whole school and form. • External agencies – e.g. Bully Busters, Brave the Rage	New initiative to be rolled out summer 2018 by DS/CR online ambassadors.	MOG and subject staff MOG and subject staff MOG and subject staff AF/DS /CR GL/CC CR/TA's/Subject staff CR/DS/AF KP and SEN team/CR RK/AF/CR CR/DS –new initiative
Get the opportunity to improve their digital literacy skills?	• In ICT/Computing lessons 7-11 • In cross- curricular lessons.		Subject staff
Are aware of the School's Acceptable Use Rules	• Accepted at login, available on intranet • AUP issued to 7 at new intake meeting and 12 autumn term • New students when join are issued a copy to sign		CR/TAs Admin Admin
Know how to report any concerns they may have?	• Clause in AUP/ • Notices in rooms state how this should be done		CR

What	Already in Place	Action Required	Person(s) Responsible
Whole School			
We have a nominated online safety co-ordinator?	• Overall responsibility for online safety lies with the Principal and this can't be delegated • The designated safeguarding lead is DS • The governor responsible for Online Safety is: P. Oliver • The Designated Child Protection Officer is RL • The e-Safety Coordinator is: CR		SBR RL ? RL CR
We have a school Online safety Policy	• Policy in place • Last updated – March 2018 • The school online-safety policy agreed by governors on: Jan 16 • The policy is available for staff at:		CR/DS
The school audits its online-safety measures?	• Reviewed annually • Agenda item at network meetings • Safeguarding on Meeting Agendas • Regular dialogue with SS/Convene and Technician		CR/Network admin SLT
Robust AUPs	• AUP staff in place – latest version incorporated in 2015-16 Online Safety Policy (This doc) Previous version Sept 09 • AUP student updated Mar 18 and in place • 2017 version Issued to new Y7 and 12		DS CR/Admin
We use a "trusted" supplier for internet services?	• Spitfire (BT) new contract as of Oct 2016		SS/Network Admin
Network and Internet use is closely monitored and individual usage can be traced?	• Monitoring software deployed- Watchguard • Audit trail kept by network administrators – IT tech can run reports from Impero classroom management sofware • Removable drive use limited esp for students • Cloud service content use monitored – one drive implementation will not take place until this drive can be viewed as a network drive	May need to re-emphasis this message on USBs	Network admin CR/Network Admin/SS

What	Already in Place	Action Required	Person responsible
ICT security audit initiated by SLT	• Audit last conducted by Network consultant, JD at Convene • Audit in 2018 initiated as part of academy procedures monitoring • Kept under review	ongoing	SS/Network Admin/JD Convene LA?
Personal data collected, stored and used according to the principles of the Data Protection Act? **GDPR from May 2018**	• All data is stored securely • Review procedures regularly • Regular letters regarding policy on this. • Admin/Finance depts aware of compliance surrounding GDPR and working towards this.	Companies that collect data on citizens in European Union (EU) countries will need to comply with strict new rules around protecting customer data by May 25.	Admin Office/Network Admin/SS/MD/CR/SD
Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. LDL)	• Internet connection provided by Spitfire (BT) • Filtering software applied by network admin and uses Watch guard system		Network Admin
Staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT	• Network Manager and technicians report directly to Vice Principal SS • DS– Assistant Principal Pastoral kept up to date with provision for this		RL/SS/ Network Admin
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	• Use Watchguard system • Additionally in school Impero software deployed • Removable storage device use limited to decrease risk of inappropriate materials being brought into school		

What	Already in Place	Action Required	Person responsible
Keep an incident log and monitor our measures?	• ICT tech keep an incident log in conjunction with RL – Pastoral Assistant Principal. • Regularly reviewed	Not sure if this is still in place	DS/ICT Tech
Handle cyberbullying issues well?	• Assistant Principal Pastoral is DSO so has responsibility safeguarding and ensures that all incidents are responded to appropriately		DS?RK/VW/Pastoral team
<u>Parents and governors...</u>			
Understand online-safety issues and risks	• The Online Safety policy is available for parents/carers at: • Available on website along with parental information • Governors have seen and approved Online Safety Policy • Governors receive regular updates		CR/DS DS/CR
Understand their roles and responsibilities?	• Parents/carers sign and return AUP that their child will comply with the School Online Safety Rules? • Info on website		CR/DS/Admin
Receive regular training and updates?	• Info on website • Letters home • Regular tweets and parentmail emails and newsletters from school • Parent event for Online safety	Last held April 2017 Need to hold an event summer term in conjunction with new initiative	CR/DS/RK
Understand how to protect their children in the home?	• Detailed in AUP • Info on website • Leaflets home/Smart talk/ • Regular tweets and emails and newsletters from school • Parents info meeting		CR