IT POLICY

DATE APPROVED BY DIRECTORS: 29TH September 2021

BOARD REVIEW DATE: 29th September 2022

COMMITTEE RESPONSIBLE FOR REVIEW: Finance and Resources

Contents

Aims

Our Lady of the Magnificat ("the MAC") aims to have robust processes in place to ensure the online safety of pupils, staff, directors, governors and volunteers. We aim to deliver an effective approach to online safety, which empowers us to protect and educate the whole MAC community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'). The MAC will establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation 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 scam

2. *Legislation and Guidance*

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (September 2021), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Principals and schools 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.

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

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

3. Roles and Responsibilities

3.1 The Local Governing body ("the LGB")

The LGB has overall responsibility for monitoring this policy and holding the Principal to account for its implementation in School.

The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The LGB Member who oversees online safety in the school.

All LGB Members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The CSEL / Principal

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

The Principal must report any online safety issues or incidents to the LGB and Catholic Senior Executive Leader (CEO).

The Catholic Senior Executive Leader (CEO) is responsible for ensuring Central Team staff understand this policy, and that it is being implemented consistently throughout the MAC.

3.3 The designated safeguarding lead ("the DSL)

Details of the school's DSL [and deputy/deputies] are set out in our Safeguarding Policy inc Child

Protection as well as relevant job descriptions.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, IT Services Lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school Safeguarding Policy inc Child Protection
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the Principal and/or Local Governing Body

This list is not intended to be exhaustive.

3.4 The IT Services Lead

The IT Services Lead is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the MAC / School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the MAC / School's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff, directors and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the MAC / School's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here' This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre https://www.saferinternet.org.uk/

Hot topics – Childnet International https://www.childnet.com/ Parent resource sheet – Childnet International https://www.childnet.com/parents-and-carers/ Healthy relationships – Disrespect Nobody https://www.gov.uk/government/collections/disrespect-nobody-campaign

3.7 Visitors and members of the community

Visitors and members of the community who use the MAC / School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. *Educating Pupils about Online Safety*

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

All schools have to teach:

Relationships education and health education in primary schools

Relationships and sex education and health education in secondary schools

4.1 Applicable to Our Lady of the Magnificat Primary schools In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies Pupils in Key Stage 2 will be taught to:
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact By the end of primary school, Magnificat pupils will know:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

4.2 Applicable to Our Lady of the Magnificat Secondary schools In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns Pupils in Key Stage 4 will be taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, Magnificat pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. *Educating Parents about Online Safety*

The MAC / School's will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
Online safety will also be covered during parents' evenings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. *Cyber-bullying*

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The MAC / School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, directors, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
The MAC/School also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the MAC/School will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

MAC/School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element. Any searching of pupils will be carried out in line with:

The DfE's latest guidance on screening, searching and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

The MAC/School's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the MAC/School complaints procedure.

7. *Acceptable use of the Internet in Our Lady of the Magnificat*

All pupils, parents, staff, directors, governors and volunteers are expected to sign an agreement regarding the acceptable use of the MAC/School's ICT systems and the internet (appendices 1-3).

Visitors will be expected to read and agree to the MAC/School's terms on acceptable use if relevant.

Use of the MAC/School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

9. *Staff using Work Devices Outside Our Lady of the Magnificat*

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the MAC/School's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

10. How the MAC/School's will Respond to Issues of Misuse

Where a pupil misuses the MAC/School's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the MAC/School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedure and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The MAC/School's will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Directors and Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in the MAC safeguarding policy including Child Protection.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Chief Finance and Operations Officer. At every review, the policy will be shared with the directors, local governing bodies, Principals and School Staff. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other Policies

This online safety policy is linked to our:

- Safeguarding policy including child protection
- Schools' Behaviour policy
- Staff disciplinary policy and procedures
- Data protection policy and privacy notices
- Complaints procedure
- Referenced to KCSIE (Sept 21)

Annexe 1 Staff Acceptable Use Policy

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use academy 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 will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will 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 academy ICT systems (e.g. laptops, email etc) outside of the academy.
- I understand that the academy 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 in the e-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 will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using academy 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 and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the academy website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the e-safety policy)
- I will only use chat and social networking sites in school in accordance with the academy's policies. (see section A.3.2 of the e-safety policy)
- I will only communicate with pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the e-safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and Worcestershire County Council have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy (see section A.3.1) and then with the same care as if I was using academy equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems except in an emergency (A.3.2).

- I will not open any attachments to emails, unless the source is known and trusted, 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 academy policies
- 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 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, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy 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 Academy / LA Personal Data Policy. I understand that where personal data is transferred outside the secure academy network, it must be encrypted.
- I will not take or access pupil data, or other sensitive academy data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or 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 academy 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.

When using the internet in my professional capacity or for 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 academy:

- I understand that this Acceptable Use Agreement applies not only to my work and use of academy ICT equipment in the academy, but also applies to my use of academy ICT systems and equipment out of the academy and to my use of personal equipment in the academy or in situations related to my employment by the academy.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and/or other relevant bodies including, in the event of illegal activities, the involvement of the police (see section A.2.6).

Annex 2 – Student Acceptable Use Policy

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission).
- I will keep my own personal information safe, as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others.
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows.

Pupil Acceptable Use Agreement Form

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Annexe 3 – Staff Social Networking Agreement

Social Networking - Staff Agreement

For the protection of yourself, your school community, and your establishment:

Our Lady of Lourdes Catholic MAC understands the benefits of using Social Media for personal and professional reasons for colleagues. This guidance outlines the Multi-Academies expectations for staff.

For your Safety:

- Ensure that you take necessary precautions to ensure privacy settings are set to 'Friends Only' or Private depending on the type of account and content within.
- Consider what information you have in your bio, or about me section and your profile picture, as these are often public when posts are not.
- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove from the internet.
- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.
- Do not accept pupils (even those that have recently left the school)
- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

The Safety of those in our care:

- Do not post or upload photographs relating to colleagues, pupils or parents without explicit consent. Objection to such posts can cause friction in your school and make your working environment uncomfortable.

Using Social Media for CPD and networking in a professional capacity.

The Multi Academy understands the CPD and networking benefits of using some social media website. We encourage staff to share positive experiences and shared knowledge with the wider community. I

- Where posting information that may (either through that post, or previous post/information on your profile) be identifiable about your place of work do not use social networking sites in any way that might bring your professional status, colleagues, pupils, profession, other professionals into disrepute.
- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on social networking sites, inform your line manager.
- Personal accounts cannot claim to be representing the Multi Academy or its schools. You must make clear from your content/profile that your account is your account and not the views of the Multi Academy.

Creation of accounts that are Work Social Media Accounts

The Multi-Academy encourages good communications with parents, communities, and networks by using Social Media. We recognise the positive news and interactions gained from Social Media share with the wider community the work of the trust. If you choose to represent the Multi Academy with an official account, you should:

- Discuss with your Line Manager that you are creating the account, agree on the name to indicate this is an organisation account.
- All Social Media accounts that are 'work' accounts and not your private accounts (for example accounts in the school/academy name or on behalf of a subject or element of academies) are property of the Multi Academy Company. All login details therefore need to be logged with Lourdes IT upon creation, and any subsequent updates.
- When representing the MAC online and engaging with fellow users, staff must act with the same professionalism expected when engaging in person.
- Any photos or content posted onto Social Media must follow GDPR guidance, and those identifiable in the photo or content must have given explicit permission to be shared on each social network.

- *I understand the implications of using social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.*
- *I understand that injudicious use of social networking may lead to disciplinary action.*
- *I agree to take all possible precautions as outlined above.*

Name		*Date:*
Signature		

Annexe 4 – Staff Device Agreement

You have been allocated a device, but it will remain the property of the Multi Academy and you will eventually have to return it to us. As it will remain the property of the Multi Academy, please will you indicate your acceptance of the conditions below by signing one copy of this form and returning it to the central HR Team

- The device will be covered by the school insurance if you keep to these guidelines:
    - When not in use it must be locked up or secured appropriately.
    - It must never be left in an unattended vehicle.
    - When it is being kept at your home, it must be kept out of sight (i.e. not where it could be viewed through a window).

  If you do not keep to the above guidelines, you (or your own insurance) will be liable for replacement of the device if it is lost or stolen.

- You must return the device to the Multi Academy when instructed, in good condition.

- If we ask you to return the device to the school for any reason, you must do so. You will be given reasonable notice of this (At least 24hrs).

- The warranty details will be kept by Lourdes IT - In the event of a problem, please do not attempt to repair the device or have it repaired yourself. The device must be returned to Lourdes IT who will take appropriate action.

- You are required to take good care of the device. If repair is necessary due to negligence, you will be required to meet the cost of the repair.

- The device must never be taken abroad without prior consent from the Headteacher and insurance company if required.

- The school is not responsible for the purchase of peripheral devices (printers etc.), consumables or internet costs from home.

- The device should not be loaned to other individuals or *Students* (e.g., family members or friends).

- You agree to abide by the MACs "Acceptable Use Policy (AUP)" at all times when using the device – be it at home or at school. A copy is available from HR

- You are expected to have the device in school with you daily and to use it in lessons to aid with your duties.

Annexe 5 - Data Security Policy

This document outlines requirements for staff members when accessing sensitive personal data via our computer or remote systems.

Generally, staff will access and use data which holds information on individual students on a regular basis. The ICO defines personal data as:

"Information which relates to an identifiable living individual. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews."

Some staff will have access to more sensitive personal data - *usually* in the MAC MIS System (Bromcom) and pertaining to staff and students. This data relates to things such as race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. This information may also be in other locations, such as emails and documents.

Staff will also be working with confidential documents, that whilst not containing personal information, could be confidential or only for use within the MAC or specific recipients.

Some staff may have access to administrative controls.

Our precautions on all data and systems access:

We ensure all data is securely stored in physically locked rooms with recorded access or on appropriate external systems with significant security, and that only the right people have access to the right data or administrative controls. To enforce this, staff are only permitted to use the details given to them to log in to the network or external services and are to abide by the MAC AUP.

Individual users should only ever use their login details to access systems. These user accounts are setup with the correct access. Where further access is deemed necessary, this will be applied on a per user basis.

Accessing/Sharing Data

The MAC requires information to be shared within the Office365 platform wherever possible – both internally and externally.

All staff must use Multi Factor Authentication on any accounts where it is available.

All emails containing any personal information are required to be sent via encrypted systems.

Taking data off site
Staff may only take ANY data offsite if data is stored on an encrypted Multi Academy managed laptop or device.

Accessing information off site
Staff should use Office365 to access data remotely. Staff are not permitted to store MAC data locally on any non-school device.

It is staff's responsibility to:

- Ensure their PC or Laptop has up to date security software installed on it if a personal device.
- Lock their PC or device when left unattended.
- Ensure their user access to any personal devices is not shared with others.

- Be aware of the content they are viewing/sharing with others and consider the MAC Privacy Policy and other relevant policies when sharing.
- Keep their username and password secure, not written down or easily guessable and to not share them with anyone or allow anyone to use a PC or Laptop logged in as them.
- Lock or log off their PC or Laptop when not in use or when staff leave the vicinity of the device
- Be aware of what they are projecting or have open which other staff or students may see.
- Not send emails with student's names in the subject line.
- Be aware of who they are sending data to, and if it is the correct way to transfer that data.
- Not send confidential data via email to any private email account they may hold.
- Request MFA is turned on for their accounts if they are processing sensitive personal information
- To ensure any confidential items are not stored onto a personal device.