THE FEDERATION OF ST. EDMUND'S & ST. PATRICK'S

SOCIAL MEDIA & ACCEPTABLE USE POLICY

AGREEMENT FOR STAFF

We come to a Roman Catholic School and so believe that Jesus was born, died and rose again for everyone. We aim to help, encourage and show God's way to our families, making sure that our Catholic traditions and faith are kept alive. Each year at school, we learn a little bit more about our faith so that we can grow to love God and each other more.

At our schools, we seek at all times to be a witness to Jesus Christ. We remember this when putting our policies into practice. Therefore this pay policy will reflect the Catholic identity and mission of our schools and the values it proclaims.

The federation of St. Edmund's & St. Patrick's is committed to safeguarding and promoting the welfare of children and expects all governors, staff, parents and volunteers to share this commitment.

OBJECTIVES

IT (including data) and the related technologies such as e-mail, 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 IT. This policy sets out the federation's policy on social networking & the acceptable-use of IT devices. Social networking activities conducted online, outside work, such as blogging, involvement in any social networking sites such as Facebook, Twitter, Instagram, Snapchat etc and posting material, images or comments on sites such as Youtube can have a negative effect on an organisation's reputation and image.

In addition, the federation has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites and the acceptable use of electronic devices.

KEY PRINCIPLES

- Everyone (governors, staff, students, volunteers, visitors, parents) at our schools has a responsibility to ensure that they protect the reputation of the schools and to treat colleagues and members of the federation with professionalism and respect which is line with our mission statement and staff code of conduct.
- It is important to protect everyone at the schools from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is paramount and is a key responsibility of all members of staff and it is essential that everyone in the federation considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.

- With safeguarding in mind, staff and visitors invited in by the schools are asked not to use their mobile phones in public areas around school. This is to protect adults and children.
- This policy relates to social networking outside work. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorized by the Executive Headteacher. A list of these sites are listed later in this document.
- It is also completely unacceptable to communicate on social media about the schools or any member of the schools' communities in or out of work on personally owned equipment.

AIMS

- To set out the key principles and code of conduct expected of all members of staff, governors, visitors and volunteers at the federation with respect to social networking and acceptable use of IT.
- To strengthen and further safeguard and protect our children and staff.

OVERVIEW AND EXPECTATIONS

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children, the public in general and all those with whom they work.

Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting. The guidance contained in this policy is an attempt to identify what behaviours are expected of staff who work with children.

Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential to the Designated Safeguarding Lead or a member of the Safeguarding team.

The school, via our IT providers (One Education) control access to social media and social networking sites in school and regularly monitor website usage. Any issues or suspected misuse is reported to the Executive Headteacher. The school also uses a 24-hour online monitoring service provided by 'Smoothwall, Visigo' which monitors text analysis on all school hardware, including lap-tops and i-pads issued to staff. Visigo provide a weekly report to the Executive Headteacher highlighting any cause for concern and whether further action is required.

All staff are aware of the Data Protection policy and access regular training on GDPR. In line with our Data Protection policy, personal data can only be taken out of school or accessed remotely when authorised by the Executive Headteacher. Teachers, the School Business Manager and the Administrator Co-ordinator have the authority to do this and have been issued with laptops which are encrypted.

ACCEPTABLE USE SPECIFIC TO SOCIAL NETWORKING

The federation considere the following as unacceptable use of social networking:

- Under no circumstances should staff make reference to any staff member, governor, pupil, parent, visitor or school activity/event.
- The use of the schools' name, logo, or any other published material without written prior permission from the Executive Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the schools to any form of illegal conduct or which may damage the reputation of the individual school or federation. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the schools. *(If in doubt about whether something is or isn't confidential – the advice from the federation is that all school matters and business are confidential and should not be discussed or referred to with anyone unless in a professional capacity.)*
- The posting of any images of employees, children, governors, staff or anyone directly connected with the school whilst engaged in school activities.

In addition to the above, everyone in the federation must ensure that they:

- Communicate with children and parents in an open and transparent way using the school phone number and email address.
- Never 'friend' a pupil in the federation onto their social networking site.
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the schools, or anyone at or connected with the schools.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the schools' reputation is compromised by inappropriate postings.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Make sure that high levels of privacy are set if they choose to use social media.

Potential and actual breaches of the social media & acceptable use policy

In instances where there has been a breach of the above acceptable use policy, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this may result in action being taken under the federation's disciplinary procedure.
- A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the federation's mission and mission into practice.
- The governing body will take appropriate action in order to protect the schools' reputation and that of its staff, parents, governors, children and anyone else directly linked to the federation.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered in this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Executive Headteacher (or in their absence, one of the Deputy Headteachers) of the justification for any such action already taken or proposed. The Executive Headteacher will in turn see advice from One Education HR department and or the Authority Designated Officer (ADO) where appropriate. This policy takes account of employment legislation and best practice guidelines in relation to social networking and acceptable use in addition to the legal obligations of governing bodies and the relevant legislation.

ACCEPTABLE, SAFE ONLINE BEHAVIOUR AND CONDUCT

Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the federation, the profession, the diocese or the local authority.

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for children or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties. All staff, particularly new staff, should review their social networking sites when they join the federation to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the federation if they are published outside of the site.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children or other individuals connected with the federation or another school, Salford diocese or local authority could result in formal action being taken against them. This includes the uploading of photographs which might bring the federation into disrepute.

MOBILE PHONES

To ensure the safety and welfare of children in our care, personal IT devices, including mobile phones must not be used when children are present.

- All mobile phones must be kept in a secure place (not in a pocket), switched off and not be accessed throughout time with children.
- Any conversations and or communication using a mobile phone must take place out of sight and ear-shot of children and preferably other adults. Both schools have plenty of rooms that are allocated to staff only.
- In exceptional circumstances, an employee may have to have their phone on for a 'one off' occasion. This needs to be discussed and agreed with either the Executive Headteacher or one of the Deputy Headteachers.
- 'Smart' watches are to be used as watches. Staff are expected to use them as a watch throughout their time with children and not use it to access their phone.
- Employees need to ensure that they have given family members their school's phone number in case of emergencies.
- Photographs or images of any children within our care may only be taken following parental consent and only using one of the school issued i-pads. These images should only

be used for school use and teachers have the responsibility to delete photographs regularly, once they have served their purpose.

- Personal mobiles cannot be used to record classroom activities or collect evidence for curriculum coverage – e.g. drama, P.E., Art and Music. ONLY school issued i-pads can be used for this. It is the class teacher's responsibility to ensure that evidence is collected using the school issued i-pads. When external providers are used to teach specialist subjects, it is the responsibility of the class teacher and subject leader to ensure that the necessary evidence is collected using the school-issued i-pads.
- During school visits, mobile phones should be used away from children and for emergency purposes only.
- During school visits or sporting events, staff must only use school-issued i-pads to take photographs.

PROTECTION OF PERSONAL DATA & INFORMATION

Staff should not give their personal data or information to children or parents. This includes their phone numbers or personal email addresses. Any communication with parents must be made via the school offices or admin email address. Staff should also be very careful about any other personal information they give to children and parents during conversations – this might include their age, address details of their social life. This is information that could be misconstrued and does not safeguard the employee. There will be occasions when there are social contacts between children and staff, where for example the parent and teacher are part of the same social circle or members of the same parish or community. These contacts however, will be easily recognised and openly acknowledged. Staff have a responsibility to make any such contact known to the Executive Headteacher or in their absence, one of the Deputy Headteachers.

Under no circumstances should employees accept invitations to family social occasions such as birthday parties or 1st Holy Communion celebrations.

Staff should never share their work log-ins or passwords with other people, including colleagues. Staff should change their passwords regularly and this is done by the federation's IT providers. However, they should also do this for their school email address. No member of staff is allowed access to any other employee's email account. If this happens by accident because a colleague hasn't logged out, the employee is expected to log out of the account before opening their own. Accessing another employee's email account, laptop or computer without permission will be seen as a breach of this policy and governors will follow disciplinary procedures. One Education IT department monitor staff usage of IT and report any concerns to the Executive Headteacher. All employees have a responsibility to ensure that the IT equipment and access is secure.

All staff have responsibility to safeguard children and staff. If a member of staff suspects that anyone is accessing someone else's email account or having an inappropriate relationship with a pupil or family, they must report their concern immediately to the Executive Headteacher, or in their absence, one of the Deputy Headteachers, following the whistleblowing policy. Failure to do so is in breach of this policy.

Access to inappropriate images and internet usage

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the materials themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, the Executive Headteacher, or in their absence, one of the Deputy Headteachers, should be informed and that person will seek advice from One Education HR department and the ADO (Authority Designated Officer). The school will not attempt to investigate or evaluate the material themselves until such advice is received.

All staff have responsibility to safeguard children. If a member of staff suspects that anyone is accessing inappropriate images or use of the internet, they must report this immediately to the Executive Headteacher, or in their absence, one of the Deputy Headteachers, following the whistleblowing policy. Failure to do so is in breach of this policy.

CYBER-BULLYING

The federation's definition of cyber-bullying is, *'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate and individual in the attempt to gain power and control over them.'*

In order to reduce the potential for cyber-bullying, children are not allowed to use their phones in school. Following consultation and conversations with parents, it is agreed that our older children who make their own way to and from school, may bring their phone to school if their parents so wish. In these circumstances, the child takes their phone to the school office each morning where is held for safe-keeping. They collect their phone at the end of the day. The teachers will speak to the children about how to use their phone and keep themselves safe when they are travelling to and from school.

Prevention activities are key to ensuring that staff are protected from the potential threat of cyber-bullying. All employees are reminded of the need to protect themselves from the potential threat of cyber-bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyber-bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or emails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the website.

Staff should follow the federation's anti-bullying policy and procedures and the Executive Headteacher and Deputy Headteachers should be informed so they can provide the necessary support to the pupils, staff and parents. In all instances, the anti-bullying policy and procedures must be followed. All instances of bullying are reported to the governing body.

The federation's anti-bullying policy, e-safety policy and acceptable-use policy for children are reviewed with pupils on an annual basis.

All staff are expected to sign this policy and adhere at all times to its contents.

- I will always log off my computer/lap-top when I finish using it.
- I will always put a security lock (ctrl/alt/delete) on when I leave my computer/laptop unattended.
- I will take the necessary care of any school-issued device and understand that it is my responsibility to look after it.
- I will ensure that I have the adequate and appropriate home insurance if I take the school-issued device home.
- I will only use the school's email, internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher and Governing Body.
- I will comply with the IT 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 not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that I adhere to and comply with the school's data protection policy.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that I comply with the school's data protection policy when handling any personal data and ensure that all school work is undertaken on a school issued device or an encrypted USB.
- I will ensure that I comply with the school's whistleblowing policy and follow the necessary procedures if I have concerns about another member of staff and their use of IT.
- I will not share my password with colleagues, pupils or parents unless at the request of the Executive Headteacher or Governing Body for investigation purposes.
- I will not install any hardware or software.
- 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, guardian or staff member. Images will not be distributed outside the school network without permission of the parent/guardian, member of staff or Executive Headteacher.
- Images of pupils and/or staff will be deleted once they have been used for purpose.
- I understand that all my use of the internet and other related technologies is monitored and logged and can be made available, on request, to the Executive Headteacher or governing body.
- 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.
- I understand that email or text communication with a child outside of agreed protocols, may lead to disciplinary and/or criminal investigations.
- I have read and understand and agree to adhere to 'Keeping Children Safe in Education' part 1(September 2019).

In addition:

- I will not have any communication with pupils on social networking sites. Although you may not be close to a person on your 'friends' list the connotation of the word friend is strong and this must be considered when making a choice on who to accept.
- I understand that the Governing Body strongly advises that I do not have communication with any parents from our schools on social networking sites.
- I will keep up to date with the latest guidelines, policies and procedures for Acceptable-use E-Safety and social media.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Personal publishing and on-line communication will be taught via age appropriate sites that are suitable for educational purposes. They will be monitored by the school.
- All members of the school community, in line with other policies are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- News groups will be blocked unless a specific use is approved.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/guardians who will be reminded of our e-safety policy.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.

Staff use of personal devices:

- I will ensure I follow school policy regarding how and when I use my mobile phone to access my school email account, facebook, twitter and CPOMs.
- I will be the only person to access these accounts from my phone and I will ensure I have the necessary security and settings in place.
- I will ensure that when accessing these accounts, I am doing so for school business and I am away from other people.
- I fully understand the implications if I choose to have access to these accounts from my phone.
- I will not use my own personal phone or device for contacting children, young people and their families within or outside of the setting in a professional capacity.
- I will use the school phone where contact with pupils or parents/guardians is required.
- I will not provide any child with my personal contact details including my mobile telephone number.
- I will not request, or respond to, any personal information from a child other than that which is appropriate as part of my professional role.
- Once in school, I will switch my mobile phone and device to "silent" mode and bluetooth communication should be "hidden" or switched off.
- I will not use my mobile phone or other personal IT devices during working hours/contact with children unless permission has been given by the Executive Headteacher or in her absence one of the Deputy Headteachers in emergency/extenuating circumstances.
- My mobile phone will not be kept about my person, i.e. in my pocket or at my work station during working hours. I will put it somewhere safe (class stock room, school office, staff room, office drawer) and out of reach of pupils.
- I will not use any personal device such as a mobile phone or camera to take photos or videos of pupils and will only use school-issued equipment for this purpose.

- I understand that if I choose not to adhere to this policy, then disciplinary action may be taken.

List of social media sites that staff will access for curriculum and school use:

- Facebook
- Twitter
- Instagram
- Snapchat
- Musicly

Review of policy

Due to the ever-changing nature of information and communication technologies, it is best practice that this policy is reviewed and updated annually.

User Signature

I agree to follow this Social Media & Acceptable Use policy and support the safe and secure use of IT & personal data throughout the school. I understand my responsibility and the accountability.

Staff signature ____ Date _________________________

Full name ____ (printed)

Links to other federation policies and DfE guidance:

Safeguarding & Child Protection
Whistleblowing
Equal opportunities
Anti-bullying
E-safety
Staff code of conduct
'Keeping Children Safe in Education' Sept 2019
Teaching online safety in school June 2019
Data Protection
Privacy notices for children & workforce
Equality
Safer Recruitment