ACCEPTABLE USE POLICY

St Philip Westbrook C of E Aided Primary School

Date of Review	Action
MAY 2016	Agreed with Governors
MAY 2017	

1. INTRODUCTION

1.1 The purpose of this policy is to define acceptable use of the computing facilities of the School in conjunction with its established culture of ethical and lawful behaviour, openness, trust and integrity. This Policy is based upon Warrington Borough Council Acceptable Use Policy for Schools.

1.2 These facilities are provided to support the vision, objectives and services of the School and must be used and managed appropriately to assure the confidentiality, integrity and availability of the information for which we are responsible.

2. SCOPE

2.1 All employees, contractors, 3rd party users, shared service users or anyone undertaking work on behalf of the School or accessing School/Warrington Borough Council (WBC) Information and Communication systems must adhere to this policy. This policy applies to all information assets owned or leased by the School, or to devices that connect to the School network or any WBC networks and services.

2.2 This policy is not exclusive and must always be read in conjunction with the schools E Safety Policy.

3. EXCEPTIONS

3.1 Any exceptions to this policy must be agreed in advance by the Headteacher.

4. AUTHORISATION

4.1 In order to make use of the computing facilities of the School you must first be authorised to do so. Authorisation is conditional upon acceptance of this Acceptable Use Policy. Subsequent to successful authorisation, a username, and password will be created for you; and access will be given to the computing resources.

4.2 All individually allocated usernames are for the exclusive use of the individual to whom they were allocated. You are personally responsible and accountable for all activities associated with your username. Under no circumstances must your password ever be divulged; the only person who needs to know it is you.

4.3 Attempting to access or make use of any username for which you are not authorised to use, is prohibited. You must not use another person's username or password to log onto the computing resources. You may not use, or attempt to make use of, computing resources allocated to another person, unless explicitly authorised to do so by the owner of those resources. You will be responsible for any activity undertaken under your username.

4.4 You must correctly and truthfully identify yourself at all times and must not attempt to impersonate anyone else, withhold their identity or tamper with any audit trail. You must take all reasonable precautions to protect your identity. Failure to do so may be regarded as a breach of this policy.

5. PRIVACY, MONITORING AND FILTERING

5.1 Right to Privacy

5.1.1 It is accepted that the private lives of employees can, and usually will extend into the workplace. Consequently, to ensure your right to privacy, all monitoring activities will be governed by the Data Protection Act 1998 and the Human Rights Act 1998.

5.2 Monitoring

5.2.1 The School/WBC does not generally engage in systematic monitoring and recording activities. However, it reserves the right to do so where there is reason to believe that misuse of its information assets or computing facilities is occurring. Any individual using the information assets or computing facilities of the School/WBC consents to such monitoring and recording.

5.2.2 If apparent criminal activity is detected, monitoring logs, in conjunction with specific personal information, may be provided to the Police.

5.3 Filtering

5.3.1 The official school e-Mail service and Internet service are both automatically filtered to ensure that inappropriate and unauthorised content is minimised as far as is possible without detracting from either service.

6. SCHOOL REPRESENTATION & CONDUCT

6.1 When using the computing facilities of the School you must act in accordance with any school policies; to help the School maintain a reputation for quality and integrity.

6.2 Employees who are aware of any impropriety, breach of procedure, unlawfulness or maladministration, should report this to their Headteacher/Chair of Governors.

7. INTELLECTUAL PROPERTY

7.1 All information stored within the computing facilities of the School or WBC is the property of the School/WBC and may be accessed at any time where there is a need to ensure compliance with legislation and internal policy.

8. CONDITIONS OF USE

8.1 All users of the computing facilities of the School/WBC must abide by the following standards of acceptable and ethical use and must not act in such a way which would bring the school into disrepute:

Acceptable

- You must only use the computing facilities which you have been authorised to access;
- You must protect the confidentiality, integrity and availability of information;
- You must respect the privacy and personal rights of others;
- Your use of the School/WBC computing facilities must at all times comply with the law and the copyright and intellectual property rights of others;
- All users must comply with the Data Protection Act and ensure that any data handled or processed is accordance with the principles.
- Where you are aware of a data breach or security incident, you must report this to ICT via the appropriate channels.
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files. Personal USB devices should not be used.
- You should only use your personal mobile phone at break times or lunch times where there are no children present, during other times mobile phones should not be to hand. (For example they should not be used for telling the time etc) Employees must understand that, if they do use their own mobile in school, they will follow the rules set out in this agreement, in the same way as if they were using school equipment.
- You must keep personal phone numbers and email accounts private and not use your own mobile phones or email accounts to contact pupils.
- You should only use a school mobile phone when on a school trip, personal mobile phones should not be used when children are present.

Non- Acceptable

- You must not use either the school/Council facilities or any other personal computing facilities to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person;
- You must not use the facilities for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material;
- You must not use facilities for any kind of commercial activity personal gain or conducting political activities;
- You must not install or distribute software for which you do not have a licence or copy any School/WBC provided software
- You must not use social networking sites to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the School into disrepute;

- Social networking sites must not be used for party political purposes or specific campaigning purposes which 'in whole or part appears to affect public support for a political party' (LGA 1986);
- Social networking sites must not be used in an abusive or hateful manner;
- Social networking sites must not be used for unwanted communication that causes fear, alarm or distress.
- You must not befriend/follow pupils or former pupils under the age of 18. (Any exceptions should be discussed with the Headteacher)
- It is advised not to befriend/follow family members of pupils, governors or church clergy, ex pupils or ex parents on social networking sites.
- You should not post information and photos about yourselves, or school-related matters, publicly that you wouldn't want employers, colleagues, pupils, parents and other school stakeholders to see;
- You must not send sensitive or personal data in any format without it being appropriately protected and secured.

You should refer to the associated 'Acceptable Use Policy Guides' listed in Appendix A for further direction and specific examples including:

- Acceptable Usage Policy- Guidance on the use of social networking, blogs and communities
- Dealing with a security incident

These guides and other related policy guidance can be found at http://wired.

9. PERSONAL USE

9.1 Personal use of the computing facilities of the School should not take place.

9.2 Employees who take portable computing facilities home as part of their role, may use them for their personal use, taking into consideration the standards of acceptable and ethical use as given in section 8. Employees must not allow any unauthorised person access to school computing facilities at any time.

9.2 The School reserves the right to withdraw access to its computing facilities for this category of use at any time.

9.3 You must not use either personal or School supplied equipment to:-

- publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages.

- to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person;

10. INVESTIGATION OF VIOLATIONS AND CORRECTIVE ACTION

10.1 Where it is believed that a user has failed to comply with this policy, the violation will be investigated and the individual may be subject to the School's disciplinary procedure. Access will be withdrawn if an employee is found to be downloading information without the appropriate licence.

10.2 Any breach found to be substantiated may be considered in line with the School's Disciplinary Procedure.

10.3 In cases of potentially criminal content, the Headteacher will consider whether the police and/or the LADO should be involved, following appropriate liaison with HR.

11. NOTIFICATION AND ACCEPTANCE

11.1 All individuals who have been granted the right to use the School's/Council's computing facilities understand and accept this policy and supporting documentation through the terms and conditions of their contract.

12. FURTHER INFORMATION

12.1 Further advice and guidance on this policy or specific circumstances covered by this policy can be obtained from your dedicated HR Business Partner.

12.2 If you would like to comment on the content of this policy, please contact the HR Advisory Team 01925 442941.

12.3 This policy is also available in alternative formats such Braille, large print, on audio tape or community languages if requested.

Appendix 1 Information Security Management

Acceptable Usage Policy Guide- Email

1. Introduction

Use of email by school employees is permitted and encouraged where such use supports the goals and objectives of the school.

However, in order to protect the school and its information and data, the organisation has an acceptable usage guide for the use of email whereby the employee must ensure that they:

- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary risk to the school by their misuse of the service.

2. Scope

All school employees, contractors and partners are obliged to adhere to this document. The AUP guide applies to all information and communications facilities owned or leased by the school/WBC, or to devices that connect to school or WBC network..

3. Unacceptable Behaviour

All school, contractors and partners must ensure that they behave in line with conditions of use within the Acceptable Usage Policy.

Examples of unacceptable behaviour which is in conflict with the guidance includes, but is not exclusive to the following:-

- School/WBC email and communications systems must not be used to set up personal businesses, undertake personal or non-school business or send chain letters
- Confidential and sensitive messages or data must not be sent OR forwarded through email to external locations or email addresses unless a secure and encrypted method is used. Warrington Borough Council will be subject to fines from the Information Commissioner's Office if a data breach occurs through unsecured email.
- The email and communications systems must not be used for distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- use the email and communications systems for distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- The email and communication systems must not allow access to copyrighted information in a way that violates the copyright
- breaking into School/WBC's or another organisation's system or attempt unauthorised use of a password/mailbox

- using the email and communications systems for broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- using the email and communications systems for transmitting unsolicited commercial or advertising material
- using the email and communications systems for undertaking deliberate activities that waste staff effort or networked resources
- introduction of any form of computer virus or malware into the corporate network through the email and communications systems

4. Monitoring

All of the company's email resources are provided for business purposes. Therefore, the school/WBC maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the school/WBC also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.

Appendix 2 Information Security Management

Acceptable Use Policy Guidance- Internet

5. Introduction

Use of the Internet is permitted and encouraged where such use supports the goals and objectives of the school.

However, in order to protect the School and its information and data, the School has an acceptable usage guide for the use of the internet whereby employees, contractors and third parties who have access to School information systems, must ensure that they:

- Comply with current legislation;
- Use the internet in an acceptable way;
- Do not create unnecessary risk to the School by their misuse of the internet.

6. Scope

The AUP guide applies to all access of the internet from information and communications facilities owned or leased by the School/Warrington Borough Council (WBC), or to devices that connect to a WBC or School network or reside at a School/WBC site such as PC, laptop or smartphone.

7. Unacceptable Behaviour

Examples of unacceptable behaviour which is in conflict with the guidance includes, but is not exclusive to the following:-

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material;
- Using a computer to perpetrate any form of fraud, or software, film or music piracy;
- Using the internet to send offensive or harassing material to other users;
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- Hacking into unauthorised areas;
- Publishing defamatory and/or knowingly false material about the School, your colleagues, parents, pupils and/or citizens on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format;
- Undertaking deliberate activities that waste employee effort or networked resources;
- Introducing any form of malicious software into the School network.

8. Council Owned Information Held on Third Party Websites

If you produce, collect and/or process School owned information in the course of your work, the information remains the property of the School. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Appendix 3 Information Security Management

Acceptable Usage Policy Guide on the use of Social Networking, Blogs & Communities

9. Introduction

There is an increased recognition of the benefits of using social networking, blogs and online communities for business usage. This guidance sets out the best practice of using these as part of the School community to ensure that the confidentiality, integrity and availability of our data and information systems stays protected.

10. Scope

This document covers the use of social networking applications by school employees, and by partners or other third parties (including contractors) on behalf of the school.

The requirements of this document apply to all uses of social networking applications which are used for any school related purpose and regardless of whether the applications are hosted by school or not.

Social networking applications include, but are not limited to:

- Blogs, for example Blogger and Wordpress
- Online discussion forums, such as Ning
- Collaborative spaces, such as Wetpaint
- Media sharing services, for example YouTube
- 'Microblogging' applications, for example Twitter.

The principles of this AUP guide also apply to other types of online presence such as virtual worlds and RSS aggregation services and the use of these services should be in line with these policy requirements.

All school employees should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

11. Purpose

The purpose of this AUP guide is to ensure:

- that the School is not exposed to legal and governance risks;
- that the reputation of the School is not adversely affected;
- that our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the School.
- That sensitive or confidential data is not posted onto forums, blogs, communities or other social networking sites

12. Guidance and Recommendations

4.1 Use of social networking applications which are not related to school (for example, contributing to a wiki provided by a professional association) must still operate in line with the requirements set out in section 4.2 and 4.3.

4.2 School employees must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all School employees. This includes, but is not limited to, public facing applications such as open discussion forums and internally facing uses such as project blogs regardless of whether they are hosted on School/Council networks or not.

4.3 Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. The School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

4.4 Users need to be aware of accidentally bringing the workplace or professional role into disrepute through inadvertently posting inappropriate comments about work, criticising School/council or government policy and even fellow employees. Comments made online are not safe and secure and should never be considered as such.

13. Social Media Acceptable Behaviours

The acceptable behaviours include, but are not exclusive to the following:-

- do be aware that anyone can access the internet and the content you post on there, consider the level of personal information that you have available
- do remember that even if you delete content, due to the way information is easily copied and replicated, it may still be available to find on the internet
- social media must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute;
- must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- must not be used in an abusive or hateful manner;
- must not be used for unwanted communication that causes fear, alarm or distress;
- must not breach the School's misconduct, equal opportunities or bullying and harassment policies;
- Where individuals from partner organisations are involved and are acting on behalf of the School, they will also be expected to comply with the relevant school policies.

14. Using the School Logo

It is also important to ensure that members of the public and other users of online services know when a social networking application is being used for official School purposes. To assist with this, all School employees must adhere to the following requirements:

- they must only use @warrington.gov.uk or school email addresses (or that of their own reputable organisation if they are not employed by the school/Council) for user accounts which will be used for official School purposes;
- the use of the school's logo and other branding elements should be used where appropriate to indicate the school's support. The logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- School representatives should ensure that any contributions they make are professional and uphold the reputation of the school;
- School/council representatives must not promote or comment on political matters or issues that may be regarded as such.

Appendix 4 Information Security Management

Acceptable Usage Policy Guide- Email

15. Introduction

Use of email by school employees is permitted and encouraged where such use supports the goals and objectives of the school.

However, in order to protect the school and its information and data, the organisation has an acceptable usage guide for the use of email whereby the employee must ensure that they:

- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary risk to the school by their misuse of the service.

16. Scope

All school employees, contractors and partners are obliged to adhere to this document. The AUP guide applies to all information and communications facilities owned or leased by the school/WBC, or to devices that connect to school or WBC network..

17. Unacceptable Behaviour

All school, contractors and partners must ensure that they behave in line with conditions of use within the Acceptable Usage Policy.

Examples of unacceptable behaviour which is in conflict with the guidance includes, but is not exclusive to the following:-

- School/WBC email and communications systems must not be used to set up personal businesses, undertake personal or non-school business or send chain letters
- Confidential and sensitive messages or data must not be sent OR forwarded through email to external locations or email addresses unless a secure and encrypted method is used. Warrington Borough Council will be subject to fines from the Information Commissioner's Office if a data breach occurs through unsecured email.
- The email and communications systems must not be used for distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- use the email and communications systems for distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- The email and communication systems must not allow access to copyrighted information in a way that violates the copyright
- breaking into School/WBC's or another organisation's system or attempt unauthorised use of a password/mailbox
- using the email and communications systems for broadcasting unsolicited personal views on social, political, religious or other non-business related matters

- using the email and communications systems for transmitting unsolicited commercial or advertising material
- using the email and communications systems for undertaking deliberate activities that waste staff effort or networked resources
- introduction of any form of computer virus or malware into the corporate network through the email and communications systems

18. Monitoring

All of the company's email resources are provided for business purposes. Therefore, the school/WBC maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the school/WBC also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.