OUGHTRINGTON
COMMUNITY
PRIMARY SCHOOL

Acceptable Use Policy

(ICT Facilities & Information Security)

Oughtrington Community Primary School

Lymm

Cheshire

WA13 9EH

Version	Date	Action
1	February 2017	Updated Policy
2	May 2018	Updated Policy

Users of this document are responsible for familiarising themselves with the latest version on a regular basis. You should be aware that a physical copy might not be the latest available version.

Approved by:	TBC	**Date:**	TBC
Authorised by:	JCC	**Date:**	TBC
Issued by:	Governance & Security Team	**Date:**	TBC
Change Forecast:	Changes are expected at each annual review to account for changes in legislation, technology and practice.	**Review Date:**	TBC
Circulation:	All (Schools)		

Change History

Version	Authorised by	Date	Summary of Changes
2.0.1	N/A	18/06/2015	Full review and update
2.0.2	N/A	01/09/2015	Updated following feedback from HR and Information Governance Group
2.0.3	N/A	11/09/2015	Updated following consultation with Trade Unions
2.1	JCC	22/10/2015	Final version
2.2	TBC	08/03/2018	Full review and update (including use of revised document template)

Contents

INTRODUCTION **4**

1 Who does the Acceptable Use Policy Apply to? **5**

1.1 Responsibilities of Headteachers & Governors 5

2 Privacy, Monitoring and Filtering **5**

2.1 Privacy 5

2.2 Monitoring 5

2.3 Filtering 6

3 Intellectual Property **6**

4 'Sensitive Information' **6**

PRINCIPLES OF ACCEPTABLE USE **7**

5 General Principles **7**

5.1 School Representation & Conduct 8

6 Usernames and Passwords **8**

7 Use of Council School ICT Equipment **9**

7.1 Laptop, Tablet & Smartphone Users 10

7.2 Personal use of Council Equipment and ICT Facilities 11

7.3 Secure Disposal of Council ICT Equipment 11

8 Use of Personal & Non-Council ICT Equipment **11**

9 Sharing, Sending & Storing Information **12**

9.1 Information Classification 12

9.2 Using e-mail to send Sensitive Information 12

9.3 Using Removable Media to store Sensitive Information 13

9.4 Cloud Services 13

10 Internet, Email & Social Media **14**

10.1 Email 14

10.1 Social Media 14

11 Security Incidents **15**

APPENDICES **16**

Appendix 1 – Guidance Examples of Security Incidents **16**

Appendix 2 – Examples of Security Incidents **17**

Appendix 3 – Passwords - Good Practice Guidance **18**

INTRODUCTION

A school collects, hold and uses information that is both confidential and valuable. Such information and the computer systems that store, process and transmit it must be adequately protected against any activity that could affect authorised and lawful use.

It is also important that the use of ICT resources is regulated, to ensure that a school complies with relevant legislation, regulatory codes of practice, its own governance arrangements and ICT & Information Security best practice. This policy has been developed to set standards and provide users with clear instructions and guidance on what constitutes acceptable and unacceptable use. Should issues arise, staff and head teachers may wish to liaise with trade unions at an early stage, who can provide guidance documents with specific scenarios which may be helpful.

Where Warrington Borough Council, 'the Council', provides ICT services and/or ICT infrastructure to the School, it is also important that Council facilities are protected.

In brief, the aims of the Acceptable Use Policy (AUP) are to:

- Protect School staff, users and the School's equipment and the information assets we hold;
- Prevent the abuse or misuse of computer, internet, e-mail facilities and paper files;
- Prevent information security incidents and/or information loss and breaches;
- Ensure compliance with legislation;
- Where applicable, protect the Councils ICT Facilities.

This policy should be read in conjunction with the relevant Schools policies, procedures and guidance.

Key Message
All users must be aware of their obligations under this policy and take reasonable action to ensure on-going compliance. As a condition of use, it is the responsibility of users to ensure that they keep up-to-date with the latest requirements of the policy.

1. WHO DOES THIS ACCEPTABLE USE POLICY APPLY TO?

This policy and any references to 'the school' or 'users' refer to, but are not limited to, teachers and all other school staff, agency workers, contractors, 3rd parties and temporary staff such as work placements.

1.1 Responsibilities of Head Teachers & Governors

Head Teachers and/or Governors will support this AUP by:

- Implementing the Policy within the school and ensuring that the AUP is circulated to all personnel;
- Ensuring that staff understand the legal risk and security implications of improper use of school ICT facilities;
- Promoting good information security practice, by leading by example and ensuring they adhere to the conditions within this policy;
- Defining, with their team, the acceptable level of personal use of school and personally owned hardware such as mobile phones and facilities such as personal email accounts etc.

Head Teachers and/or Governors must ensure that the ICT facilities utilised by their school are configured and operated appropriately to protect the information held within or accessed by them. Guidance on the use of Cloud Services, 'Bring Your Own Device' and End User Devices (PCs, Laptops, Tablets, Smartphones, etc.) is available in Appendix 1.

2. PRIVACY, MONITORING & FILTERING

2.1 Right to Privacy

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.

All reasonable measures will be undertaken to ensure that personal emails marked as such will not be opened in the course of monitoring unless there is a legal requirement to do so or there is suspicion that email has been used in a way that would constitute gross misconduct under their contract of employment.

2.2 Monitoring

The School (and/or Council if applicable) 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.

Nevertheless, the school (and/or Council if applicable) 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 (and/or Council if applicable) also reserves the right to use monitoring software in order to check upon the use and content of emails.

Key Message
Any individual using the information assets or computing facilities of the school consents to such monitoring and recording. If apparent criminal activity is detected, monitoring logs, in conjunction with specific personal information, may be provided to the Police.

Such monitoring is for legitimate purposes only and will be undertaken in accordance with the procedure agreed with employees.

2.3 Filtering

For Schools taking the Council's e-mail and Internet services, they are both automatically filtered to ensure that inappropriate and unauthorised content is minimised as far as is possible without detracting from either service.

3. INTELLECTUAL PROPERTY

Schools own the copyright in the information they produce. Copyright may also be assigned or transferred to an individual or organisation by the original owner(s). All information stored within the ICT facilities of the school and may be accessed at any time where there is a need to ensure compliance with legislation and internal policy.

4. SENSITIVE INFORMATION

The term 'sensitive information' is used in a variety of contexts and can have different meanings according to the relevant legislation or usage.

In the context of this Acceptable Use Policy, 'sensitive information' includes any information which requires protection from unauthorised or unwanted loss or disclosure. This will typically include, but is not limited to:

- Personal data (including client records; staff records, appraisals, disciplinary cases, etc.);
- Sensitive personal data (for example, health records)

- Bank and payment card information;
- Research or other proprietary information;
- Commercial data, leases, contracts, etc.;
- Information marked as 'OFFICIAL – SENSITIVE';
- Any information where loss or disclosure could lead to damaging consequences for an individual or group of individuals; damage the reputation of the School, compromise ICT security or cause the School to not fulfil its statutory obligations.

PRINCIPLES OF ACCEPTABLE USE

5. GENERAL PRINCIPLES

The School's ICT facilities must only be used by those authorised to do so. Any user who requires access to School ICT facilities must first:

- Be authorised to do so by a manager, supervisor or sponsor;
- Read, understand and accept all relevant School policies and this Acceptable Use Policy.

You must not deliberately or knowingly use the School's ICT facilities to view, copy, create, download, share, store, print, e-mail, transfer or otherwise access any material which:

- Is sexually explicit or obscene;
- Is racist, sexist, homophobic or in any other way discriminatory or offensive;
- Contains content where the possession, transmission or sharing of would constitute a criminal offence;
- Promotes any form of criminal activity;
- Brings the School into disrepute and/or exposes it to legal action.

It is unacceptable to use the Schools ICT facilities to:

- Conduct any non-approved business;
- Undertake any activities detrimental to the reputation of the School;
- Make offensive or derogatory remarks about anybody on social media or otherwise via the Internet or e-mail;
- Create, transmit, download or share information, or install software or applications, which would breach copyright, confidentiality or any other applicable legislation;
- Impersonate or attempt to impersonate another individual or organisation;
- Attempt to gain access to information or information systems you are unauthorised to access;
- Attempt to bypass internet filtering or any monitoring functions;
- Attempt to conceal your identity by using anonymising software or services;

- Deliberately or knowingly undertake activities that corrupt or destroy School data, disrupt the work of others, deny network resources to them or violate the privacy of other users.

5.1 School Representation & Conduct

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

Employees who are aware of any impropriety, breach of procedure, unlawfulness or maladministration, should report this to their Head Teacher or Line Manager**.**

Key Message
Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people. Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

6. USERNAMES & PASSWORDS

Authorised users will be issued a username, password and, where necessary, an e-mail address. All log on and account information, including your password, is provided for your exclusive use only.

Don’ts

- ***For usernames allocated to a single user:***

        - You must not share any usernames, passwords, access tokens or ID badges with any other user as you alone are responsible for any activities undertaken under your details;
    - ***For usernames allocated to two or more users:***
        - You must not share any usernames, passwords, access tokens or ID badges with any other user, other than those who have been approved as part of their role to access it;
    - You must not write down or display your password;
    - You must not store passwords for any School system in any automated logon or within a website where it asks to save your password;
    - You must not store your username, password or other credentials within any website including web based e-mail accounts such as Yahoo or Gmail;
    - You must not attempt to access or make use of any username or e-mail address that is not your own;
    - You must not attempt to impersonate anyone else;
    - You must not leave your PC unlocked. Ensure that you lock your PC before leaving your desk;
    - You should not use a password which contains a single dictionary word (e.g. Orange123) as these have been demonstrated to be very easy to 'crack' or discover.
        - Further guidance on choosing stronger passwords is available in *Appendix 3* of this document.

Useful Information
Ideally, your password should must be: ▪ A minimum least 8 characters long; ▪ Comprised of at least three of the four types of characters (upper case, lower case, numbers and symbols); ▪ Changed if you believe that your password has been compromised or if you suspect that someone else knows your password; ▪ Different from the last 20 passwords you have used. **Your password should not:** ▪ Contain a single dictionary word (e.g. Orange123).

7. USE OF SCHOOL ICT EQUIPMENT

Any equipment supplied to you (for example, Laptops, PCs, Smartphones, Tablets) remains the property of the School at all times, with the user assuming temporary 'custodianship'.

Do's

- Make sure that at all times you use this equipment in accordance with this Acceptable Use Policy, securely, for the purpose for which it was issued to you, without reconfiguration and in compliance with relevant legislation such as the Computer Misuse Act 1990 and Data Protection Act 1998[1] ;
- On leaving employment with the School, you must ensure that all ICT equipment is returned to your line manager or the Head Teacher;
- Before you store any films, music or other media on ICT equipment, ensure that you are aware of your responsibilities under the current intellectual property legislation. Guidance can be found here;
- Report the loss or theft of any ICT equipment to your School;
- Ensure that your screen cannot easily be viewed by others when accessing sensitive information. For example, if you were working away from Schools premises or in a public area.

7.1 Laptop, Tablet and Smartphone Users

All School ICT equipment is subject to information security risks, but the portability of laptops, tablets and smartphones makes them particularly vulnerable to damage, loss or theft, either for their re-sale value or the information they contain. When outside of secured premises, there is an increased risk to any laptops or portable devices that you may carry as part of your role.

Do's

- Users must keep ICT equipment in their possession within their sight whenever possible. ICT equipment should never be left visibly unattended unless it is suitably secured (for example in a secure office or using a "Kensington lock");
- Extra care should be taken in public places such as airports, railway stations or restaurants;
- When transporting ICT equipment, you should look to minimise the risk of loss or theft. For example, putting a laptop out of sight in the boot of a car rather than on the passenger seat;
- You must ensure that the device is regularly connected and logged onto the network to receive its security updates;
- You must ensure that laptops are regularly restarted to ensure that all security updates are applied;
- Any data saved to the device is not backed up centrally. You should avoid saving data to the device wherever possible. However, where this is necessary for operational reasons you must ensure that data on the device is backed up to the network storage areas for your School as soon as is practical.

[1] The Data Protection Act is due to be replaced/superseded by the General Data Protection Regulation (GDPR) with effect from 25th May 2018.

Don'ts

- If a device is secured either with an encryption password or a 'lock screen' password, you must not share your encryption / lock screen password with anyone or write this down.

7.2 Personal Use of School Equipment & ICT Facilities

Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of the School's/Council's e-mail and Internet systems may result in disciplinary action.

School devices contain or enable access to school data and systems. Personal use of school ICT equipment does not extend to other family members, friends or any other person, unless they are formally authorised to do so (See Section 5).

7.3 Secure Disposal of School ICT Equipment

School ICT equipment which is broken, no longer fit for purpose, redundant or to be used/donated for other purposes should be securely wiped (where applicable) and disposed in-line with WEEE regulations.

Don'ts

- You must not sell or donate School equipment to staff, charities or any other third-parties without the explicit authorisation of the Head Teacher and/or the School Governors.

8. USE OF PERSONAL AND NON-SCHOOL ICT EQUIPMENT

The use of non-school and personal ICT equipment to undertake school business brings both opportunities and risks. The potential for an increase in flexibility and convenience must be balanced against the need to keep personal and sensitive information secure.

- You must only use your personal hand held/external devices (mobile phones/USB devices etc.) in School if permission has been gained. (Schools may amend this section in the light of their mobile phone and/or hand held devices policies if appropriate). Employees must understand that, if they do use their own devices 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 must only use a School mobile phone when on a school trip

NOTE: Schools should also document their policy on the use of Personal and Non-School ICT equipment here (e.g. Laptops, PCs, etc.). Links to Guidance on 'Bring Your Own Device' are available in Appendix 1.

Useful Information
Non-School and personal ICT equipment includes: ▪ Personal smartphones, tablets, laptops, PCs, networking equipment or other devices; ▪ Devices from partner organisations, government agencies, businesses, citizens, contractors, etc.

9. SHARING, SENDING & STORING INFORMATION

9.1 Information Classification

During the course of its business, a School sends and receives large quantities of data. Not all of this will be personal or sensitive, but if you handle (create, send, receive, etc.) such data, then you need to be aware of how to look after it.

Some information will be labelled with a *classification* (e.g. Official, Sensitive, Confidential etc.) which identifies how sensitive it is. However, much of the information you handle will not be labelled.

Key Message
You will need to use your professional judgement, in conjunction with available guidance, practice and processes to ensure that you are aware of the sensitivity of the information you work with. Any sensitive information must be handled (sent, stored, etc.) appropriately.

9.2 Using e-mail to send sensitive information

Do's

- You must use appropriate technology to encrypt or otherwise protect e-mail containing sensitive information if you are sending it outside of the School.

9.3 Using Removable Media to Store Sensitive Information

Removable media can be a convenient way to store and share information.

Do's

- Ensure that all files on the removable media are also stored on School drives or within ICT systems - removable media can be lost or damaged;
- Ensure that any unwanted or faulty removable media are disposed of in an appropriate and secure manner.

Don'ts

- Do not store sensitive information on removable media that is not encrypted (for example, standard USB memory sticks, CDs, tapes, SD cards).

Useful Information
Removable Media incudes: ▪ CDs and DVDs; ▪ USB memory sticks and external hard drives; ▪ Memory cards (e.g. SD cards) and SIM cards; ▪ Digital cameras, MP3 players; ▪ Backup tapes, audio cassettes.

9.4 Cloud Services

The terms 'cloud services' or 'the cloud' cover a number of technologies which provide access to software, applications, data and ICT infrastructure (typically) over the Internet. For example, services such as Dropbox offer file storage; Office 365 allows access to e-mail and Microsoft Office applications.

The UK Government and the Information Commissioner's Office (ICO) have issued guidance about the use of 'Cloud' solutions. It is recommended that schools use this guidance to assess the technical, security, governance and legislative impact of any Cloud Service. Links to this guidance can be found in Appendix 1.

Do's

- Make use Cloud-based technologies approved by your School for sharing information and collaborating;

Don'ts

- You must not store any sensitive School information in a cloud service which has not been formally assessed and approved by the School for that purpose.

10. INTERNET, EMAIL & SOCIAL MEDIA

The internet, e-mail and social media are all important channels used by a School to share, publicise and access information.

Key Message
Remember that the **General Principles** outlined in **Section 5** of this document apply when you are using the Internet, e-mail or social media.

10.1 Email

Do's

- Check that you have selected the correct e-mail addresses(s) before you send every message;
- If you receive e-mail not intended for you, notify the sender and then delete the original;
- Ensure that any sensitive information sent by e-mail is adequately protected. See *Section 9.2* ***Using e-mail to send sensitive information*** for further information.

Don'ts

- You must not use, disclose, distribute, copy, print or forward any information contained in an e-mail which has been sent to you in error;
- If you receive an e-mail from an unknown source ('spam' e-mail) do not open any attachments or click on any links. Don't forward the e-mail and don't reply to the sender (as this may attract further e-mails).

10.2 Social Media

Although this Acceptable Use Policy applies to the use of School facilities, it is important to note that the use of social media outside of work can affect the workplace. For example:

- Comments posted on social media may be seen by work colleagues, and a private disagreement may 'spill over' into the workplace.

Do's

- Follow the general principles outlined in Section 5. of this document;

Don'ts

- 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.
- You must not befriend pupils on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils);
- Do 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;

11. SECURITY INCIDENTS

Security Incidents, for example the theft of a laptop, a computer virus or a successful hacking attack could compromise the security of School. A successful compromise may:

- Affect business operations;
- Lead to financial loss or reputational damage;
- Be a threat to the personal safety or privacy of an individual or organisation;
- Need to be reported to the UK Government, the Information Commissioner's Office, Police or a number of other organisations.

Examples of events that may result in a security incident occurring are available in *Appendix 2* of this document.

Do's

- Ensure you report all security incidents to the school, and if necessary, to the Council's ICT Service via 2200.

Don'ts

- Don't ignore a security incident assuming that someone else will report it.

APPENDIX 1 - Guidance

I. Information Commissioner's Office

Bring your own device (BYOD) guidance
Cloud computing – Guidance

II. National Cyber Security Centre (NCSC)

End User Device Security
Bring your own device

APPENDIX 2 – EXAMPLES OF SECURITY INCIDENTS

The following are examples of security incidents:

- Damage to or theft/loss of information (either manual or electronic)
- The finding of confidential information/records in a public area
- Poor disposal of confidential waste
- Unauthorised access to information
- Unauthorised disclosure of confidential information to a third party (in any format including verbally)
- Transfer of information to the wrong person (by e-mail, fax, post, or phone)
- Receiving of information (such as by e-mail or fax) meant for someone else
- Sharing of computer IDs and passwords
- Loss or damage to paper based files containing sensitive or personal identifiable information
- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. CD, USB stick
- Corrupted data
- Access to inappropriate websites in breach of policy
- Theft
- Fraud
- A computer virus
- Successful hacking attack
- Any other breach of the data protection act or other relevant legislation

APPENDIX 3: PASSWORDS – GOOD PRACTICE GUIDANCE

I. Choose a password that cannot easily be guessed – avoid using the names of children, partners, pets, car registration numbers or favourite football/rugby teams. This is information that could relatively easily be uncovered by social engineering techniques, looking at the electoral register, etc.

II. Some passwords are easy to discover or 'crack' using simple techniques known as dictionary or brute force attacks. These include passwords using dictionary words, e.g. Orange123.

a. Consider longer phrases, rather than single words:

i. For example, **Beesmaketastyhoney!**

b. Substitute letters for numbers and symbols or add further numbers/symbols. For example, rather than rather than **Oranges123** you could use:

i. **Or954ang£s123** (Orang£s123 with the number 954 inserted in the middle to break up the word);

ii. **s3gn@rO321** (Or@ng3s reversed, 123 reversed)

NOTE: These are just 2 examples – it is important you find a formula or format that you can remember and works for you.