Polehampton C. of E. Schools Federation

Online Safety Policy

Document Version:

Initial Approval Date: 28.6.12
Review Period – as required

Document History

Version	**Issue Date**	**Comments**	**Total pages**	**Signed by chair of committee**
1	28.6.12	Approved at the Curriculum Effectiveness Committee	16	
2	1.7.15	Changes made following training and revision to Wokingham model policy	21	
3	5.10.16	Added in reference to Wokingham's social media parent letter	22	
4	5.2.2020	Back up information clarified and cloud working clarified	23	

Introduction

Our Online Safety Policy addresses the full scope of current risks in relation to IT used in our school. We have included aspects of data security, password security, encryption and all aspects of risk into a single Online Safety Policy. Sections of this policy covers statutory responsibilities such as the Data Protection Act and the Computer Misuse Act as well as school based policies such as parental agreement with respect to school photography.

Alongside this policy, please refer to the staff's checklist to ensure we comply with the day to day implications of this policy.

The work of Kent County Council, Wokingham Borough Council, and Radstock Primary School, is acknowledged in providing material for this document.

1. Roles and Responsibilities

1.1 Governors

Governors are responsible for the approval of the Online Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. Governors will require/undertake the following regular activities:

- Meetings with the Online Safety Officer.
- Monitoring of Online Safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school Online Safety matters.
- Be conscious of security re: confidential school documents, i.e. Analyse school performance (see governor Online Safety checklist)

The current Safeguarding Governor is Brian Rogers.

1.2 Headteacher and SLT

The Executive Headteacher is responsible for ensuring the overall safety, including online safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (as noted in the 2018 Keeping Children Safe in Education statutory guidance). On a practical day-to-day basis, others may have particular duties relating to Online Safety e.g. an Online Safety Officer, Computing Subject Leader, Network Manager/Technician. However, the Headteacher will ensure the following:

- Staff with online safety responsibilities receive suitable and regular training, including awareness of current IT trends and risks, enabling them to carry out their online safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular monitoring reports.
- There is a clear procedure to be followed in the event of a serious online safety allegation being made against another member of staff.
- Parents are educated about online safety on a regular basis through newsletter updates, circulation of relevant magazines (Digital Parenting) and school-based presentations.

1.3 Online Safety Officer

The Online Safety Officer has day-to-day responsibility for Online Safety issues and takes a leading role in establishing and reviewing the school Online Safety Policy and associated documents. The Online Safety Officer will also:

- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provide materials and advice for integrating Online Safety within schemes of work and check that Online Safety is taught on a regular basis.
- Liaise with the local authority.
- Liaise with the school's technical staff.
- Ensure that Online Safety incidents are reported and logged and used to inform future Online Safety developments.
- Report to the governors and meet with them as required.
- Report regularly to the SLT.

1.4 IT Technician/Network Manager

The IT Technician/Network Manager in co-operation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network, ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- The IT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the Online Safety technical requirements outlined in any relevant local authority Online Safety Policy/guidance.
- Users may only access the school's network through a properly enforced password protection policy, in which passwords are regularly changed.
- The schools' filtering policy is applied and updated as appropriate and its implementation is not the sole responsibility of any single person.
- Online Safety technical information is kept up to date, applied as necessary and passed on to others where relevant.
- Use of the network and websites are regularly monitored and any misuse/attempted misuse reported to the Online Safety Officer or designated person for investigation and action.
- Appropriate steps are taken to protect personal information and secure data on all devices and removable media.
- Provide secure access to the school network from home where necessary using VPN or equivalent technologies.

1.5 PSHE Coordinator/Computing Subject Leader/Curriculum Coordinator

- Provide materials and advice for integrating Online Safety within PSHE schemes of work.
- Check that Online Safety is taught on a regular basis.

1.6 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current Online Safety matters and the school Online Safety Policy and practices.
- They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement.
- They report any suspected misuse or problem to the Online Safety Officer for investigation and action.

- Digital communications with pupils should be on a professional level and only carried out using approved school systems.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the schools' Online Safety and Acceptable Use Policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor computing activity in lessons, extra-curricular and extended school activities.
- They are aware of Online Safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- They know and follow the procedure for dealing with any unsuitable material that is found in internet searches.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.

1.7 Designated Safeguarding Lead (DSL)/Child Protection Officer (CPO)

The DSL/CPO should be trained in Online Safety issues and be aware of child protection matters that may arise from:

- Sharing or loss of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

1.8 Data Protection Officer/School Business Manager

The responsibilities of the Data Protection Officer is to:

- Act as the contact point for all Data Protection issues and queries from Data Subjects and the ICO, e.g. for Subject Access Requests, data breaches, following the agreed procedures in the Data Protection Policy.
- Maintain appropriate documentation related to data processing.
- Undertake the training necessary to fulfil their role, and ensure staff have access to appropriate training and updates.
- Monitor compliance with all aspects of Data Protection.
- Provide advice relating to Data Protection Impact Assessments (DPIA) e.g. before introducing a new data processing system.

See Appendix 1 – School and the Data Protection Act for further information.

2. Reviewing, Reporting and Sanctions

2.1 Review

- This policy will be reviewed and updated annually, or sooner if necessary.
- The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

2.2 Acceptable Use Agreements

- All users of the school computers will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.
- All users will be expected to re-sign agreements on a regular basis.
  [See 'Appendix 6 – Exemplar Acceptable Use Agreements' for further information]

2.3 Reporting

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.

[See 'Appendix 2 – Course of action if inappropriate content is found' for further information]

2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

2.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt with in line to the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

3. Communications & Communication Technologies

3.1 Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements have been made with the school.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a school mobile phone.
- Parent helpers or visitors in school and staff must ensure that they do not use their devices or send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises, they should arrange temporary cover whilst they make a call.

- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- Schools should be vigilant where mobile phones are used within the vicinity of any children. Adult helper and visitor mobile devices may normally be switched off or on silent during the times that children are present. Adults must ensure all mobile devices are password protected, so a child couldn't have access to your data or unrestricted internet.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.2 E-mail and messaging

- Staff will be informed that the use of school email or messaging accounts will be monitored.
- Staff may access personal web-based email accounts from school but **must not** use these for communications with parents or pupils.
- Under no circumstances should users use email to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils should immediately tell a staff member if they receive an offensive email or message.
- Pupils should not reveal personal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Information of a sensitive nature should not be sent by unencrypted email and the 'secure' messaging system should be used where possible.
- Staff but not pupils may use web based email accounts from school.
- The forwarding of chain letters, jokes, etc is not permitted.
- Staff should not open an email that looks "unusual", even if it's from someone they know.

3.3 Social networking

For the purpose of this policy, social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, Linked-in, Whatsapp, blogs, chat rooms, online gaming, YouTube, Skype, etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so, they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Social networking sites should not be accessed or used during the school day on school equipment.
- Staff should recognise that their existing lists of friends/contacts/followers may include people in both their private and professional lives. Staff should not create new links with parents simply because they teach their children.
- Staff should not post photographs or videos of their class or pupils on their social networking sites.
- Staff should not mention that they are a member of staff at our schools or comment on any school issue.

- Staff should check their profile settings to ensure that: no parent or pupil (or recent pupil (under 18)) is able to see material that is not public
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
- Where necessary, parents should be reminded about their own conduct and use of social media, particularly when referring to the school.
- The Schools now have a Twitter account. This is for sharing good news; it is not intended to be for discussion or to answer questions. Senior staff run and monitor the Twitter account.

[See 'Appendix 3 – Social Networking Guidance' for further information]

3.4 Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school device. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's Online Safety Guidelines.
- Pupils will receive guidance in responsible and safe use on a regular basis.

3.5 Digital and video images

Parental permission

- The schools will ensure that appropriate written permissions are obtained from a parent with parental responsibility for the taking and use of digital and video images of pupils. Such use includes the school website, website or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- If specific individual pupil photographs are to be used publicly, such as on the school website, in the prospectus or any other high profile publication, then a check should be made with individual parents for this additional use.
- Unless specific parental permission has been obtained, pupils will not be identified by name in any title or commentary accompanying digital or video images that are in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.

Storage and deletion

- All images of pupils will be securely stored in one central location.
- Where tablets, memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.
- Images taken in the school environment for purposes of identification and education are essential for performing the public task of the school so will be retained whilst the child remains at school, after that the image should be deleted in accordance with the Data Protection Policy.
- Images taken in the school environment as records of school events that make up the school's history, may be kept securely by the school in accordance with the Data Protection Policy.

Recording of images

- All staff and pupils must sign the ICT Acceptable Use Agreement.
- School digital devices should always be used to record images of pupils. Staff and volunteers should not use their own devices to take images of pupils.
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Where images are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online 'cloud' storage) care must be taken that the location of images of pupils is clearly understood and in line with ICO (Information Commissioner's Office) guidance.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Where volunteers are supporting school staff, they should abide by the same rules as school staff as far as is reasonable.
- Children are not allowed to use their own cameras in school or on trips.
- Staff and volunteers must monitor when children are using cameras in the curriculum, i.e. child-initiated time in FS or similar.

Parents taking photographs or video

Where the school allows the recording of images at in-school 'public' events such as Sports Day and plays, the following will apply:

- Images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

Events/activities involving multiple schools

- At times, the Polehampton schools may visit other schools or go on trips.
- Although the schools will make reasonable efforts to safeguard the digital images of pupils, parents will be made aware that at some types of events, it is not always realistic to strictly

enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

3.6 School website

- The school website should include the school address, school email, telephone and fax number, including any emergency contact details.
- The school website should be used to provide information and guidance to parents concerning Online Safety policies and practices.
- Learners' names may not be used on the website in conjunction with photographs.
- Staff or pupils' home information should not be published.
- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing.

4. Infrastructure and Security

4.1 Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School ICT technical staff may monitor and record the activity of users on the school IT systems and users will be made aware of this.
- Servers, and communications cabinets, should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the IT Technician/Network Manager.
- Access to the school ICT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- The 'Administrator' passwords for the school IC system, used by the IC Technician/Network Manager are also available to the ICT Subject Leader and must be stored securely in school.

4.2 Passwords

All staff are provided with an individual password. Pupils may have a group password or individual passwords for accessing the network and associated learning platforms e.g. G Suite. All users will have an individual log on to the learning platform and/or secure areas of the website. Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil.
- 'Strong' passwords should be used.

- Once a computer has been used, users must remember to log off so that others cannot access their information.
- Users leaving a computer temporarily, should lock the screen (Windows key + L or Control + alt + del).
- Passwords should be changed at regular intervals.
- In the event that a password becomes insecure then it should be changed immediately.

[See 'Appendix 4 – Password guidance' for further information]

4.3 Filtering

The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

- Changes to network filtering should be approved by the Computing Subject Leader and the IT Technician/Network Manager.
- Any filtering issues should be reported immediately to the ISP and/or SEGfL.

4.4 Virus protection

- All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.
- The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case, only dependable sources should be used.
- If staff suspect their laptop has a virus/malware or similar issue, they should seek immediate help from the ICT Technician/Network Manager.

4.5 Staff laptops/devices and flash drives

Staff laptops/devices and flash drives are likely to be taken out of school and may well contain sensitive data (see Section 3.6). Schools should encrypt staff laptops and staff should only use school provided encrypted flash drives. The following security measures should also be taken with staff laptop/devices:

- Laptops/devices must be out of view and preferably locked away overnight, whether at school or home.
- Laptops/devices should never be left in a parked car, even in the boot.
- Screensavers should be set to lock after a maximum of 15 minutes.
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

[See 'Appendix 6 – Exemplar Acceptable Use Agreements' for further information]

4.6 Personal and sensitive data

- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
- Sensitive data is any data which links a pupil's name to a particular item of information and/or the loss of which is liable to cause individuals damage and distress. Therefore, such data:
    - must be encrypted on laptops/devices and any other removable media;
    - should not be emailed between staff;
    - should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.
- Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks.
- Sensitive information should be held in lockable storage when office staff are not present.
- There is a clear procedure for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.

[See 'Appendix 5 – Sensitive & Non-Sensitive Data' for further information]

4.7 Electronic devices - search and deletion

Schools now have the power to search pupils for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

- School staff may search for any electronic devices. Two members of staff will be present.
- Senior staff members are authorised to examine and/or erase data on electronic devices.
- Data may be deleted or kept as evidence.
- Incidents will be recorded (CPOMS)

4.8 Loading/installing software

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- Only authorised persons, such as the ICT Technician/Network Manager or Computing Subject Leader, may load software onto the school system or individual computers.
- Where staff are authorised to download software to their own laptops/devices, they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

4.9 Backup and disaster recovery

The school has a backup regime which enables recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime includes:

- The use of a cloud-based location for backup of key school information via a secure encrypted online backup system, administered and maintained by the school's ICT Technician.
- Daily back-ups of servers to onsite external hard drives conducted by the school's ICT Technician.

- Automated daily reports via email confirming status of back-ups.

5. Online Safety Education

5.1 Learning and teaching for pupils

- Pupils should be encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key Online Safety messages will be included within the curriculum (e.g 'Be Internet Legends') and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of devices should be displayed in all rooms where they are predominantly used.

5.2 Staff training

- Staff will be kept up to date through regular Online Safety and data protection training.
- Staff should always act as good role models in their use of ICT, the Internet and mobile devices.

5.3 Parental support

The support of, and partnership with, parents should be encouraged. This is likely to include the
following:

- Awareness of the school's policies regarding Online Safety and Internet use; and where appropriate being asked to sign to indicate agreement.
- Practical demonstrations and training
- Advice and guidance on areas such as:
    - filtering systems
    - educational and leisure activities
    - suggestions for safe Internet use at home

Appendix 1 – School and the Data Protection Act 2018 (GDPR)

The data protection principles set out in Article 5 of the Data Protection Act 2018 include the principle that personal data shall be:

"...processed in a manner that ensures appropriate security of the personal data, including protection
against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

This means that schools must have appropriate security to prevent the personal data held (e.g. for staff, pupils and parents) being accidentally or deliberately compromised.

The implications of this for Polehampton schools will be the need to:

- Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.
- Be clear about who is responsible for ensuring information security.
- Ensure that the school has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.
- Respond to any breach of security swiftly and effectively by reporting to the Data Protection Officer.

Failure to comply with the Act could result in loss of reputation or even legal proceedings. Further guidance may be found at www.ico.gov.uk

Appendix 2 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
  - Turn off the monitor or minimise the window.
  - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
  - Ensure the well-being of the pupil.
  - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
  - Report the details of the incident to the Online Safety Co-ordinator.
- The Online Safety Co-ordinator will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

Appendix 3 – Social networking guidelines

Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a 'private' online space.

Access to social networking sites

- Social networking sites should never be accessed during timetabled lessons and other contact with pupils and not normally during school working hours.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents simply because they teach their children.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

Appendix 4 – Password guidance

This guidance is intended for those adults using school systems but is based on good practice and should also feature in the teaching of, and advice to, pupils:

- Passwords should be strong, having a mixture of lower and upper case letters, numbers and special characters. The choice of password 'strength' should be appropriate to the data being protected and the potential risks associated with that data being compromised.
- Passwords should avoid following a pattern or being predictable.
- Passwords must not be easily guessable by anyone and therefore should not include:
    - Names of family, friends, relations, pets etc.
    - Addresses or postcodes of same
    - Birthdays

    - Telephone numbers
    - Car registration numbers
    - Unadulterated whole words
- Try to use in a password:
    - A mixture of letters and numbers
    - Punctuation marks
    - At least 8 digits

Appendix 5 – Sensitive & Non-sensitive data

Sensitive data will include:

- SEN records such as IEPs, Annual Review records and EHCPs
- Mark sheets and assessments
- Reports and Open Evening comments
- Personal data stored on the school's Management Information System, e.g. SIMS
- Photographic or video material
- Name, address and contact information

Non-sensitive data thus includes:

- General teaching plans
- Curriculum materials
- General correspondence of a non-personal nature

Appendix 6 – Acceptable Use Agreements

The agreements included are:

- Parent/Carer Acceptable Use Agreement – one completed for each school
- Pupil Acceptable Use Agreement - one completed for each school
- Laptop Acceptable Use Agreement
- Staff Acceptable Use Agreement

Polehampton C.of E. Schools Children's Acceptable Use Guide

At school, we use technologies including iPads and chromebooks to learn and access the Internet. During my time at Polehampton Schools, I will be taught how to use technology and the Internet safely and responsibly.

I will learn to follow the acceptable use guide carefully as they will keep me and my fellow peers safe and happy.

- I will only share my password with my teacher and my parents.
- I will tell my teacher straight away if I think someone else knows my password.
- I will respect others work. I will not look at, edit or delete their files without their permission.
- I will not distribute images of others without their permission.
- I will only use the computers and other technology including iPads and cameras when an adult is present.
- I will always ask before I use the Internet and will only access it when an adult is present.
- When I use the Internet to research information, I should take care to check the information I find is accurate.
- I understand that images and text that I find on the Internet may have a copyright because they belong to someone else. I must consider this in my work.
- I will not bring in or use any devices of my own in school.
- I can write polite and friendly online messages to people I know with permission of an adult.
- I will be polite when I contribute to online class blogs, learning platforms and forums.
- I will not use 'text talk' when contributing to online class blogs, websites etc.
- If I receive anything I am not happy with online, or see something I shouldn't, I will tell my teacher as soon as I can.
- I will never give out any personal information on the Internet e.g. my address, phone number, date of birth or even the school I go to.
- I will never arrange to meet anyone over the Internet, even if it is a friend.
- I know that school can check anything that I do on the school computers and other technology.
- I will always try to be a good Digital Citizen and use my online world to spread positivity.
- I will respect all technology at school and will make sure that I put things back in the correct way.
- I know if I am not a responsible user then school has the right to take action. This could include a loss of access to the computers and other technologies.

I agree to follow the Online Safety rules as explained to me.

I will learn the rules whilst I am at Polehampton Schools.

Childs' Signature: …………………………………………………………… Date: ……………………

Parent's Signature …………………………………………………………… Date: …………………

Parent/Carer Acceptable Use Agreement

The school seeks to ensure that pupils have good access to ICT to enhance their learning and, in return, expects pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

===

As the parent/carer with parental responsibility of the above pupil, I understand that my child will have access to the Internet and to ICT systems at school.

I know that my child has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on school ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Child's name:	
Relationship to the child (must be a parent with parental responsibility):	
Signature:	
Date:	

Staff Acceptable Use Agreement

Please consult the school's Online Safety Policy for further information and clarification. Please use the staff checklist to inform your everyday practice.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that my school email address is used for communicating personal data and that sensitive data will be sent using secure mail.
- I will comply with the school Data Protection Policy and ensure that personal data, particularly that of pupils, is stored securely **on the school server, cloud-based locations (e.g. Outlook 365/Google) and not on the hard drive** of a PC / laptop and that this is regularly backed up to cloud based storage.
- I will ensure my password is strong and changed regularly and I will ensure that my screen is locked when inactive.
- I will only use an encrypted memory stick for transfer of sensitive files.
- I will only use my work email address when communicating sensitive data and will ensure that all confidential emails are sent using secure email.
- I will ensure that paper files containing personal data will be stored securely in school.
- I will follow the same processes for securing any paper or electronic files containing personal and sensitive data that I take off site/home.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including email, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the Internet is consistent with the school's Online Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the Internet including checking the history of pages when necessary.

- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. Online Safety Co-ordinator and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	

Laptop/Devices Acceptable Use Agreement

1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
- It should be read in conjunction with the school's Online Safety Policy
- All recipients and users of these devices should read and sign the agreement.

2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. Software

- Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
- Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. Faults

- In the event of a problem with the computer, the school's ICT Technician/Network Manager should be contacted.

Declaration:

I have read and understood the above and also the school's Online Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

Appendix 7 – Wokingham's "The challenge of social media and schools" letter

The challenge of social media and schools

Introduction

Social media (e.g. Facebook, Twitter, Instagram, etc.) has had widespread impact on the way in which we communicate and express our thoughts and opinions. There are clearly many benefits for us both as individuals and also as communities, and many of our schools are exploring how they might best harness the power of social media to engage even more closely with parents and pupils.

Unfortunately we are also experiencing an increasing number of situations where social media has been the vehicle for inappropriate behaviour by both pupils and parents.

We live in a society where we are proud of our right to freedom of speech and would not wish to suggest that this should be curtailed in any way. There are occasions however, when things said in the virtual world are at best unhelpful and, at worst, may constitute harassment, bullying or intimidation which could ultimately lead to Police involvement.

Social media and pupil bullying

There have been a growing number of situations where schools have had to deal with pupils using social media to be unkind to others. What starts as something seemingly harmless takes no account of how those on the receiving end might feel nor does it recognise how quickly things can get out of control and become extremely unpleasant.

Whilst things are most likely to have taken place off the school site and outside school hours, the resulting 'fallout' in such situations can have major implications for harmonious relationships within school and a resulting negative impact on teaching and learning.

If you have concerns that your child might be on the receiving end of hurtful social media posts, or playing a part themselves, please talk to your school in the first instance who will be able to seek additional advice and support as required.

Social media as a forum for parents' views

The staff in our schools work tremendously hard to provide the very best education for our children and always want to work in partnership with parents and the wider community. However, we recognise that there will be occasions where, for whatever reason, parents may not agree with a particular course of action or may have specific concerns.

It is entirely natural to discuss school life and express our thoughts and opinions with others face to face or on the phone. Some of these conversations are now also being aired on social media and the person posting has little control over who might ultimately see it.

Sadly, some of these comments and observations could cause offence if aired in the public domain, and may in some cases be intimidating or even slanderous. This is not to suggest that teachers and headteachers are above criticism or do not welcome feedback. However, it is always best when this is constructive and reasonable and is focused on finding an acceptable solution. When difficult things need to be said, it is usually best to do so face-to-face, or at least in some form of private communication, such as an e-mail or letter. Some recent examples of ill-considered use of social media have caused school staff to spend a disproportionate amount of time trying to manage issues and situations. We would much prefer if this time could be focused on our children's education.

Common questions

If the site I post comments on is 'private' then why should I worry what I say, as only my 'friends' can read it?

Once a comment has been posted there is nothing to stop other users forwarding or sharing it. What started as an initial 'sounding off' can quickly spread much more widely and cause a lot of unintended hurt.

How could the Police get involved?

If postings are considered to be threatening or discriminatory then the Police may become involved and have the authority to seize mobile devices and contact service providers.

How can parents help?

- If you are posting on social media and it relates to the school, pupils or other parents, please check your facts, be considerate in the way in which you express things and avoid language that others might consider to be abusive, aggressive or threatening.
- Please do not refer to individual pupils or staff on social media.
- If you have a significant concern about an aspect of school life, please talk to someone at the school before posting on social media.
- If you have a specific complaint, please follow the school's Complaints Policy which is available on the school website.

Final thoughts

We have no wish to stifle debate or discourage parents expressing their views, but want to encourage and promote positive role models in both the digital world as well as the real world. Whilst our children may be the more knowledgeable in using modern communication technologies, it is the partnership of schools and parents that can help them to use it wisely, safely and responsibly.

Ms H. Ball - Executive Headteacher - Polehampton C. of E. Schools Federation
Mrs Caroline Harrison - Chair of Governors - Polehampton C. of E. Schools Federation
Felicity Parker – Superintendent Local Police Area Wokingham Borough Council
Carol Cammiss - Director of Children's Services Bracknell & Wokingham