Beechwood Primary School

Online Safety Policy

The purpose of this policy is to:

- Set out key principles expected of all members of the whole school community at Beechwood Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Beechwood Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Reviewed: November 2019

Next review: November 2020

Head Teacher: Sally Hunter

Chair of Governors: Lester Dennis

Contents

1. Roles and Responsibilities
2. Reviewing, Reporting and Sanctions
3. Communications and Communication Technologies
4. Infrastructure and Security
5. Online Safety Education

Appendix 1 – School and the Data Protection Act

Appendix 2 – Course of action if inappropriate content is found
- Online Safety Incident Flowchart and Guidelines
- Online Safety Incident Log
- Online Safety Incident Form

Appendix 3 – Personal and social networking guidelines

Appendix 4 – Password guidance

Appendix 5 – Sensitive & Non-sensitive data

Appendix 6 –Acceptable Use Agreements
- Foundation and Year 1 Pupil Acceptable Use Agreement
- Years 2 and 3 Pupil Acceptable Use Agreement
- Years 4, 5 and 6 Pupil Acceptable Use Agreement
- Parent/Carer Acceptable Use Agreement
- Use of Digital/Video Images Agreement
- Laptop/Devices Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Pupil/Parent Mobile Phone Agreement

Appendix 7 – Social Media: Age Restrictions, Global Social Media Prism

Appendix 8 – Communications Technologies

Appendix 9 – Unsuitable / Inappropriate activities

Appendix 10 - School Actions & Sanctions

Roles and Responsibilities

1.1 Governors

Governors are responsible for the approval and work on the development of the Online Safety Policy, ensuring that it is implemented and review its effectiveness. In fulfilling this responsibility the governing body delegates day to day responsibility to the Headteacher. The Governors will undertake the following regular activities:

- Monitoring of Online Safety incident logs.
- Reporting to relevant governor committees annually or sooner if required.
- Keeping up to date with school Online Safety matters.

1.2 Headteacher

The Headteacher is responsible for ensuring the safety, including online safety, of members of the school community. The Headteacher will ensure the following:

- Staff with online safety responsibilities receive suitable and regular training enabling them to carry out their online safety roles and to train other colleagues as necessary.
- There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff.

1.3 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, understood and signed the school's Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Online Safety Officer for investigation and action.
- Digital communications (e-mail/Twitter) 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 school's 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 ICT 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.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.

1.4 Child Protection Officer (CPO)

The CPO must be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers

- Potential or actual incidents of grooming
- Online bullying

1.5 Data Protection Officer (DPO)

The DPO (School Business Manager) are responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk. SLT should be informed where school policies may require updating.

[See *'Appendix 1 – School and the Data Protection Act'* for further information]

2. Reviewing, Reporting and Sanctions

2.1 Review

- This policy is reviewed and updated bi-annually or sooner if necessary.
- The school audits 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 sign agreements when starting with the school or upon transition, when their agreements have expired.

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

2.3 Reporting

- The school produces clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers must 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 must 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 in line with 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 and Communication Technologies

3.1 Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school.
- Where mobile phones are allowed in school they must be turned off before entering the school gates and may not be used during lessons or on school premises. The sending of abusive or inappropriate text messages or images is forbidden.
- 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 a main school telephone (cordless permitted) and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- Mobile phones must not be used in any meeting including staff meetings.
- Parent helpers in school and staff must ensure that they do not 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 through approved systems during lesson times if these are part of the curriculum.
- Staff, helper and visitor mobile devices should be switched off or on silent during the times that children are present. They must not be used in the presence of pupils.
- 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

- Pupils and staff will be informed that the use of school e-mail or messaging accounts will be monitored.
- Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils may only use approved e-mail or message accounts on the school system.
- Pupils must immediately tell a staff member if they receive an offensive e-mail or message.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff before sending.
- Information of a sensitive nature must not be sent by e-mail.

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, Instagram, Google+, Pinterest, Tumblr, Reddit, Snapchat, Secret, YouTube, Skype, Second Life, LinkedIn, WhatsApp, Vine, WeChat, Kik, blogs, chat rooms and online gaming etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so they must 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.
- Pupil use of social networking in school 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.
- The use of social networking 'tools', e.g. blogs, wikis, messaging, etc., within the school environment is both acceptable and to be encouraged.

  [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 computer. 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 school will ensure that appropriate written permissions are obtained for the taking and use of digital and video images of pupils. Such use could include the school website; social media (Twitter); display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- Parental permission is to be attained annually.
- Pupils will not be identified by name in any title or commentary accompanying digital or video images that is 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 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.
- Digital images may be retained for up to 2 years after a pupil has left the school and are then deleted in line with the data retention policy.

Recording of images

- All staff and pupils must sign the relevant Acceptable Use Agreement.
- School digital devices should always be used to record 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 Commission'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.

Use of staff personal devices

Staff personally owned devices (e.g. staff smartphones, cameras, tablets) must not be used to record images, video or voice.

Parents taking photographs or video

Where the school chooses to allow the recording of images at 'public' events the following should 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

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
- Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event 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.

[See *'Appendix 6 – Use of Digital/Video Images Agreement*]

3.6 School website

- The school website should include the school address, school e-mail, 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 practice.
- 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 ICT 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 ICT Technician.
- 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 ICT system, used by the ICT Technician are also available to the Computing Co-ordinator 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. 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 or a supply teacher.
- 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).
- 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 Research Machines (RM), the Internet Service Provider, and the South East Grid for Learning (SEGfL).

- Changes to network filtering should be approved by the Online Safety Officer and the ICT Technician.
- Any filtering issues should be reported immediately to the Online Safety Officer.

4.4 Virus protection

- All computer systems, including staff laptops/devices, are protected by an antivirus product which is administered centrally and automatically updated.

4.5 Staff laptops/devices and memory devices

Staff laptops/devices and memory devices are likely to be taken out of school and may well contain sensitive data (see Section 3.6). The school password protects all staff laptop hard drives and staff must 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.
- Admin screensavers should be set to lock after a maximum of 15 minutes of inactivity.
- Teaching staff screensavers should be set to lock after a maximum of 1 hour of inactivity.
- 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 other staff are to use the laptop, they should log on as a separate user.

[See *'Appendix 6 – 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;
  - not be e-mailed between staff;
  - 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 must be clear procedures 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. Clear guidelines relating are communicated to staff and parents when needed. Such guidelines will include:

- Details of which items are banned under the school rules and may be searched for.
- A list of staff members/roles authorised to examine and/or erase data on electronic devices.
- Clear guidance as to what is, and is not, allowed when searching a pupil.
- When data will be deleted or kept as evidence.
- How incidents will be recorded.

4.8 Loading/Installing software

For the purpose of this policy, software relates to all programs, applications, 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 or Computing Co-ordinator, 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 plan

The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime includes:

- The use of a remote location for backup of key school information..
- No data should be stored on the C drive of any curriculum computer as it is liable to be overwritten without notice during the process of ghosting the computers.
- Staff are responsible for backing up their own data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.

4.10 Memory Sticks/Memory Storage Drives

No personal memory sticks/memory storage drives should be brought into school.

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 and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules regarding online safety should be displayed in each key stage corridor and be age appropriate and relevant.

5.2 Staff training

- Staff will be kept up to date through regular online safety training.
- Staff must 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 is encouraged. This should 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

[See *'Appendix 6 – Parent/Carer Acceptable Use Agreement'* for further information]

Appendix 1 – School and the Data Protection Act

The Seventh Principle of the Data Protection Act (1998) states that:
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Beechwood Primary has the appropriate level of security to prevent the personal data held (e.g. for staff, pupils and parents) being accidentally or deliberately compromised.

Appendix 2 – Course of action if inappropriate content is found

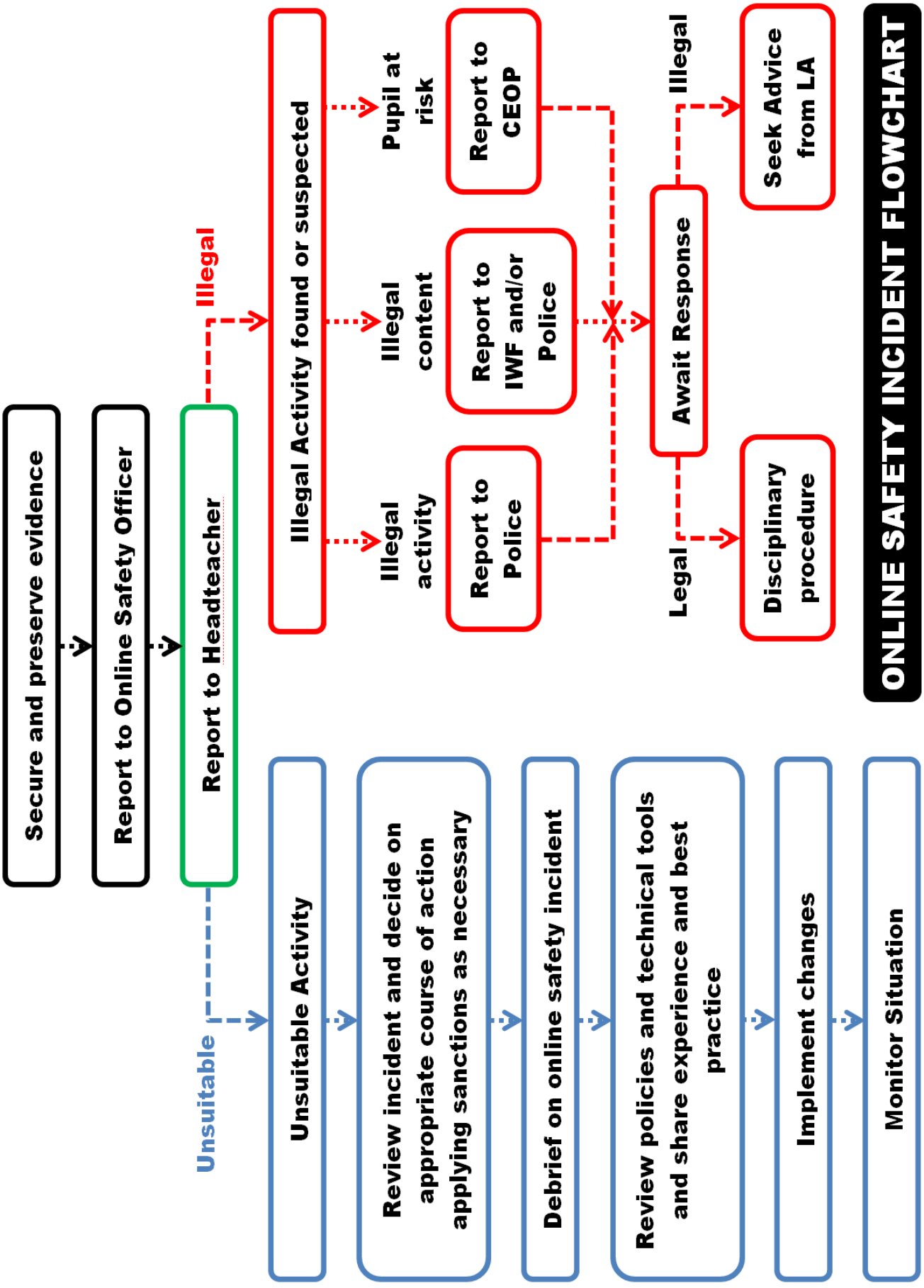
- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user must:
  - Keep the computer on and turn off the monitor or minimise the window.
  - Report the incident to the teacher or responsible adult.

- The teacher/responsible adult must:
  - 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 DSL
  - It is advisable to copy and paste the web page address and send it to the Headteacher.

- The Headteacher will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the IT provider and Internet Service Provider so that additional actions can be taken.

Overleaf is the Online Safety Incident Flowchart and set of guidelines explaining the differences between Unsuitable and Illegal Activity.

The Online Safety Incident Log and Form is to be completed in the presence of the Online Safety Officer.


ONLINE SAFETY INCIDENT FLOWCHART
Secure and preserve evidence
Report to Online Safety Officer
Report to Headteacher
Illegal
Unsuitable
Illegal Activity found or suspected
Pupil at risk
Illegal content
Illegal activity
Report to CEOP
Report to IWF and/or Police
Report to Police
Await Response
Illegal
Legal
Seek Advice from LA
Disciplinary procedure
Unsuitable Activity
Review incident and decide on appropriate course of action applying sanctions as necessary
Debrief on online safety incident
Review policies and technical tools and share experience and best practice
Implement changes
Monitor Situation

GUIDELINES

Unsuitable Activity

- Use of personal electronic device to store school related information
- Posting offensive or insulting comments
- Posting comments that affect professional standing and integrity
- Contacting pupils by email or social networking
- Pupil phone/tablet/computer used in school
- Pupils entering personal information online
- Pupils chatting online to others outside school without adult permission
- Viewing material that causes distress (if illegal, then report under Illegal Activity)
- Taking images/videos without consent
- Disclosing personal passwords

Illegal Activity found or suspected

Police (Thames Valley - Berkshire)

www.report-it.org.uk

Hatred on the grounds of your race, religion, sexual orientation, transgender identity or disability.

www.gov.uk/report-terrorism

Articles, images, speeches or videos that promote terrorism or encourage violence.

IWF - Internet Watch Foundation

www.iwf.org.uk

Child sexual abuse content hosted anywhere in the world.

Criminally obscene adult, including extreme pornography, content hosted in the UK.

Sexual abuse images of children hosted in the UK.

CEOP - Child Exploitation and Online Protection

www.ceop.police.uk

Child sexual exploitation and abuse.

Online Safety Incident Log

Date/time of incident	Name of person completing log	Date/time incident was logged	Description of incident (e.g. Nature of incident, where did it occur, who was involved: e.g. pupils, staff, parents?)	Follow up actions/further comments (e.g. evidence preserved, senior staff informed, action to prevent a recurrence)

Appendix 3 – Personal and social networking guidelines

Specific guidelines relating to staff use of social networking are detailed below:

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

- Personal social networking sites must never be accessed during timetabled lessons.
- Pupils must never be contacted / friended via social networking sites.
- Teachers may communicate with pupils via school approved social networking sites if part of the curriculum and used for teaching.
- Staff may not use school equipment to access personal social networking sites.
- If the school chooses to make 'official' use of social networking sites, such as Twitter, 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 must have a 'strength' of at least 12 where a letter is 1 and a number or punctuation mark is 2. 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 characters
  - Think of a memorable phrase such as the example below to construct a password:
    Run, **r**un **a**s **f**ast **a**s **y**ou **c**an **–** **Y**ou **c**an't **c**atch **m**e, **I**'m **t**he **G**ingerbread **M**an**!**
    A password can be constructed by using the first letter of each word and changing some letters to their digit equivalent.
    Password: Rrafayc-Yccm1tGM!
- Use a password strength checker such as https://howsecureismypassword.net/

  It would take a computer about 93 trillion years to crack the above password.

Appendix 5 – Sensitive & Non-sensitive data

Sensitive data will include:

- SEN records such as IEPs and Annual Review records
- 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 following Acceptable Use Agreements are included:

- Foundation and Year 1 Pupil Acceptable Use Agreement
- Years 2 and 3 Pupil Acceptable Use Agreement
- Years 4, 5 and 6 Pupil Acceptable Use Agreement
- Parent/Carer Acceptable Use Agreement
- Use of Digital/Video Images Agreement
- Laptop Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Pupil/Parent Mobile Phone Agreement

Foundation and Year 1 Pupil Acceptable Use Agreement

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will ask permission before I use the internet.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I have read the agreement with my child and they have understood the above and agree to follow the rules outlined.

Pupil Name:	
Parent signature:	
Date:	

Years 2 and 3 Pupil Acceptable Use Agreement

For my own personal safety:

- I understand that the school will check that I am using my computer sensibly.
- I will keep my username or password private.
- I will keep information about myself or anyone else private when online.
- I will not arrange to meet people that I have communicated with online.
- I will report anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school ICT systems are for learning and that I will only use them for playing games when I have permission to do so.

Acting as I expect others to act toward me:

- I will respect others' work and will not change, copy or remove other user's files.
- I will be polite and responsible when I communicate with others.
- I will only take or share images of anyone with their permission.

Keeping secure and safe when using technology in school:

- I will only use school e-mail or message accounts on the school system when given permission.
- I will not upload, download or access any material that I am not supposed to.
- I will immediately report any damage or faults.
- I will keep the computer settings as they are.
- I will immediately tell a staff member if I receive an offensive e-mail or message.

Using the internet for research or recreation:

- I will only use the work of others when given permission (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

I have read/had read to me the above and understand and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

Years 4, 5 and 6 Pupil Acceptable Use Agreement

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, e-mail and other digital communications.
- I will keep my username or password private and only use my own when logging into an account.
- I will keep information about myself or anyone else private when online (e.g. home address and telephone number).
- I will not arrange to meet people that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal or recreational.
- Permission must be given before the school ICT systems can be used for social media, gaming or file sharing.
- I will keep my downloads and uploads to a minimum unless I have permission.
- I will not use the school ICT systems for online gambling or internet shopping.

Acting as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only take or share images of anyone with their permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- Permission must be given before I am allowed to bring into school and use my personal handheld/external devices (e.g. Laptops, Tablets, USB devices, etc.).
- I must have a letter of permission from my parents (explaining why) before I can bring a mobile phone to school. Once I have obtained agreed permission I will hand my mobile phone in to my class teacher at the beginning of the day and it will be returned to me before I go home. The mobile phone must **be switched off before I enter the school gates** and **can be turned on after I exit the school gates**.
- I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails, unless given permission to do so and I know and trust the person/organisation that sent the e-mail.
- I will ask for permission before sending an e-mail to an external person/organisation.
- I will keep the computer settings as they are and not load software or applications.
- I will immediately tell a staff member if I receive an offensive e-mail or message.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (e.g. online bullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
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 the 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.

Parent/Carer's Name:	
Pupil's Name:	

As the parent/carer of the above pupil, I understand that my son/daughter will have access to the internet and to ICT systems at school.

I know that my son/daughter 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, as no filtering system is 100% safe.

I understand that my son's/daughter's activity on the 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.

I have read the **Pupil Acceptable Use Agreement** attached and agree that my child will abide by the rules.

Parent's Signature:	
Date:	

Use of Digital/Video Images Agreement

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school.
These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website, the school's Twitter account and occasionally in the public media.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers may be allowed to take videos and digital images of their children at school events at the school's discretion for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Parent/Carer's Name:	
Pupil's Name:	

As the parent/carer of the above pupil:

- I agree to the school taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school such as their publication in newsletters, on the school website and occasionally in the public media. **Yes / No**

- I agree to the school using the digital/video images of my child on the school's Twitter account. **Yes / No**

I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by the above guidelines in my use of these images.

Parent's 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.
- Laptops and other associated devices should never be left unattended in a vehicle at any time. Staff will be responsible for any loss in the event of theft or damage in this event.
- Staff will only use secure USB memory sticks issued by the school for saving any school documentation or work. No other forms of electronic devices will be used.
- 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

- Staff will not load onto any devices additional software without the assistance of the IT Technician or Computing Co-ordinator.
- Any such software 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 should be contacted.
- Do not attempt repairs – this will invalidate any warranty on the equipment.

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:	

Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Online Safety Policy for further information and clarification.

- 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, e-mail, 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 e-mail 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 the IT Technician.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety Policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail, 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 Officer 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 e-mail 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:	

Pupil/Parent Mobile Phone Agreement

At Beechwood Primary we are committed to providing a caring, friendly and safe environment for all our pupils and staff, and believe that modern technology in the form of mobile phones, when used appropriately, offers young people and their parents/carers peace of mind. We are also clear that when phones are used inappropriately, they distract from the core school business of learning, and at worst can be used as a tool for bullying. We understand that it is sometimes beneficial for a pupil to carry a mobile phone if they need to travel alone before or after school. We would, however, ask that pupils do not carry a mobile unless it is **absolutely essential**. If you deem that your son/daughter needs a mobile phone then you must sign the agreement below and adhere to the policies and procedures of the school:

As the pupil I understand that:

- My mobile phone should be **turned off** (not put on silent) before I enter the school gates and be put in my school bag, along with any associated accessories, and hidden from view.
- They will remain in my school bag and will not be taken out to show my friends in the playground, listen to music or any other associated activity.
- They will remain in my school bag until I enter my classroom where I will hand them to my teacher.
- I will remember to collect my phone/accessories from my teacher when I leave school that day and will put them in my school bag hidden from view.
- They will only be taken out of my bag and turned on after I leave the school gates.
- My mobile cannot be used for taking videos or photos whilst on the school premises; this includes being outside the school fences or gates. However, I may use my mobile to communicate only with my parents/carer whilst outside the school gates.
- If I do not abide by these rules my mobile phone, along with any accessories, will be confiscated and my parent/carer will be contacted. I will be asked to unlock my device in the presence of my parent/carer by the Online Safety Officer/Headteacher to examine the contents of my phone. I may then lose my privilege to bring my mobile phone to school.

As the parent/carer of the pupil I understand that:

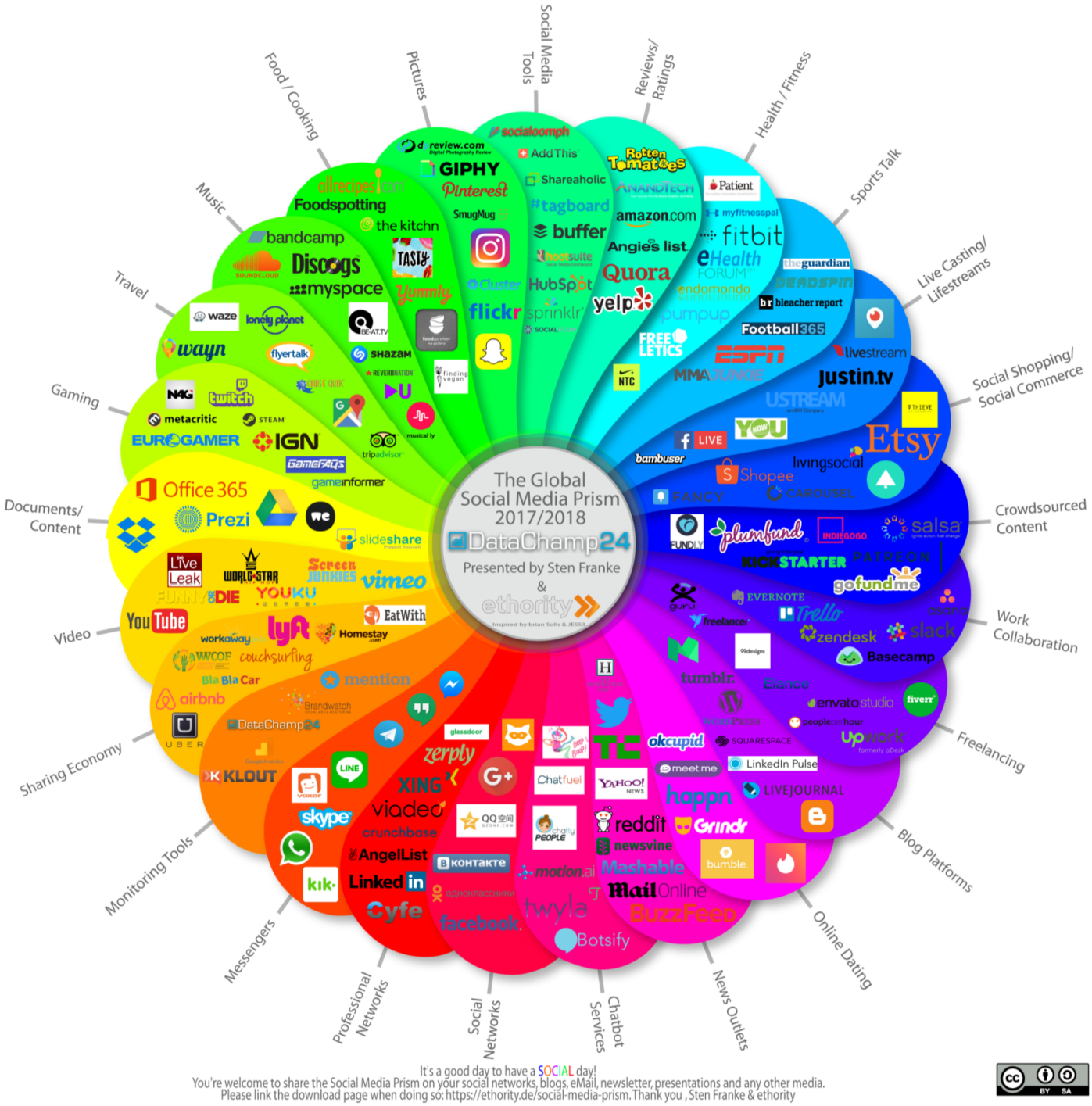
- My son/daughter is travelling to/from school without a responsible adult.
- My son/daughter will adhere to the above rules; otherwise, they may lose their privilege to bring a mobile to school.
- Whilst off the school premises, my son/daughter will use their mobile responsibly.
- The school will not be liable for any loss or damage to my child's mobile phone or its accessories.
- I will be unable to contact my son/daughter on their mobile during the school day and must use the school office number if the matter is urgent.
- I will be contacted if my son's/daughter's mobile is confiscated. In the unlikely event that I am unable to be reached the mobile will be kept by the Online Safety Officer. The data on my son's/daughter's mobile will be examined in my presence. Any data found to cause harm, disrupt teaching or that breaks the school rules will be deleted. I may give my consent over the phone for this search/deletion. However, I will still be required to collect the mobile.

Parent/Carer's Name:		Signature:	

Pupil's Name:		Signature:	
Mobile make:		Accessories:	
Mobile model:		Mobile number:	

Appendix 7 – Social Media: Age Restrictions

Appendix 7 – Social Media: Global Social Media Prism



Appendix 8 – Communications Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**	**Not allowed**
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones / cameras				✓				✓
Use of personal mobile devices e.g. tablets, gaming devices		✓						✓
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of messaging apps		✓					✓	
Use of social media		✓					✓	
Use of blogs		✓					✓	

Appendix 9 – Unsuitable / Inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008					✓
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Threatening behaviour, including promotion of physical violence or mental harm				✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✓	
On-line gaming (educational)		✓				
On-line gaming (non educational)					✓	
On-line gambling					✓	
On-line shopping / commerce			✓			
File sharing		✓				
Use of social media			✓			
Use of messaging apps			✓			
Use of video broadcasting eg Youtube			✓			

Appendix 10 – School Actions & Sanctions

The severity of the incident will be reviewed by the Headteacher and actions / sanctions applied upon a case by case basis. The table below serves as a guideline of actions / sanctions that could apply.

Students / Pupils	Actions / Sanctions								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal /Online Safety Officer	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓	✓	✓	✓	
Unauthorised use of mobile phone / digital camera / other mobile device	✓	✓	✓			✓		✓	✓
Unauthorised use of social media / messaging apps / personal email	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓	✓	✓	✓	✓	✓	✓
Allowing others to access school / academy network by sharing username and passwords	✓	✓	✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school / academy network, using another student's / pupil's account	✓	✓	✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school / academy network, using the account of a member of staff	✓	✓	✓		✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's / academy's filtering system	✓	✓	✓		✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓	✓	✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓	✓	✓	✓

Staff

Incidents:	Refer to Headteacher / Principal /Online Safety Officer	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓
Inappropriate personal use of the internet / social media / personal email	✓		✓	✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓		✓	✓	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓			✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓			✓	✓		
Deliberate actions to breach data protection or network security rules	✓			✓	✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓		✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓			✓	✓		✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓		✓	✓	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓				✓		✓
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	✓			✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓			✓	✓	✓	✓
Breaching copyright or licensing regulations	✓			✓	✓		✓