Waterfield Primary School

Computing and Online Safety Policy

September 2017

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The Counter-Terrorism and Security Act, which received Royal Assent on 12 February 2015, places a duty on specified authorities, including local authorities and childcare, education and other children's services providers, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism ("the Prevent duty"). The Prevent duty came into force on 1st July 2015. For further details, see the Child Protection Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Resources Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Computing Leader
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors during meeting

Headteacher / Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Computing Leader.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (see flow-chart on dealing with Online Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation, linked to the Prevent agenda and how to refer concerns to Channel.
- The Headteacher/Senior Leaders are responsible for ensuring that the all other staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Leader

Online Safety Coordinator/Computing Leader:

- leads the Online Safety group - See Appendix A.
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority, following consultation with the Headteacher.
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

IT Network Manager:

The IT Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required Online Safety technical requirements and any Local Authority Online Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix B)
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network/internet/DB Primary/remote access /email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader/Computing Leader for investigation /action
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

All staff are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current Waterfield Primary School Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Computing Leader for investigation/action
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety class charter and acceptable use policies
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- staff monitor the use of digital technologies, mobile devices (iPads, laptops, tablets) cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer

The Child Protection Officer should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- potential or actual incidents linked to radicalisation
- cyber-bullying

Students/pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, within DB Primary as well as beyond the school's learning platform
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, home-school diaries, the school's website, www.waterfieldprimary.co.uk or the school's learning platform DB Primary. Parents and carers will be encouraged to support Waterfield Primary School in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the school's learning platform
- the children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems/website/learning platform as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

(Appendix D - A Community Users Acceptable Use Agreement)

Policy Statements

Education – students/pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum should be provided as part of Computing lessons and should be regularly revisited
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and class activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. **Any request to do so, must be requested in writing via email, with clear reasons for the need.**

Education – parents/carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Newsletters – these will be sent out digitally (via email addresses stored in the school's information management system).
- The Online Safety section on the school's website
- The school's learning cloud – DB Primary
- Parent forum evenings / sessions – held annually
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications eg www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Online Safety
- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide Online Safety information for the wider community
- Supporting community groups e.g. Early Years Settings, childminders, youth / sports / voluntary groups, to enhance their Online Safety provision

Education & Training – Staff/Volunteers

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training, which will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- The Computing Leader (or other nominated person) will receive regular updates through attendance at external training events (e.g. from 360 degrees / CAS / LA / CEOP / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff.
- The Computing Leader (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation (e.g. e-PD).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons)

Technical – infrastructure/equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor, but it is the responsibility of the school to ensure that the managed service provider carries out all the Online Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of Waterfield Primary School's Online Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities.

(Appendix E - A more detailed Technical Security Policy)

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- The Computing Leader is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see Appendix A for more details)
- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for groups of users – staff / pupils.
- School technical staff regularly monitor and record the activity of users using and writing to the school's learning platform, DB Primary.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person whilst using the school's hardware, mobile technology or the use of the internet including the school's learning platform, DB Primary.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems – the provision here is that the ‘guest’ staff will be provided with a supply laptop from the Learning Leader which will allow the guest to access the internet and the planning folder on the shared area. The ‘guest’ users have to sign in and out the hardware.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (Appendix F - School Personal Data Policy)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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 students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website to be covered as part of the agreement signed by parents or carers at the start of each academic year.
- Pupil’s work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than is necessary
- processed in accordance with the data subject’s rights
- secure
- only transferred to others with adequate protection.

The school must ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". Please see the Freedom of Information publication hosted on the school's website.
  It has a Data Protection Policy (Appendix G – Data Protection Policy)
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- risk assessments on IT are carried out and are kept up to date
- it has clear and understood arrangements for the security, storage and transfer of personal data
- data subjects have rights of access and there are clear procedures for this to be obtained
- there are clear and understood policies and routines for the deletion and disposal of data
- there is a policy for reporting, logging, managing and recovering from information risk incidents
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- at all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption and secure password protected devices
- follow 'basic data protection' when sending out any correspondence to parents electronically– this includes electronic club registration, weekly newsletters via email etc.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies the school considers the following as good practice:

- The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service (DB Primary e-mail service for pupils) to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Through the school's learning platform, by using the 'golden whistle', pupils must report any communication that makes them feel uncomfortable.
- Any digital communication between staff and pupils (e-mail, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems, for example DB Primary. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- All pupils at KS1 and above will be provided with individual school e-mail addresses for educational use. These e-mail accounts are restricted to the SafeMail features within the school's learning platform, DB Primary.

- Pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.
- All bulk emails, sent out by the school, will comply with data protection regulations. This includes electronic club bookings, newsletters and any other letter sent out to more than one recipient.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes, a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012, while Ofsted's Online Safety framework 2012 reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training, to include acceptable use, social media risks, checking of settings, data protection and reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to students/pupils, parents/carers or school staff
- staff do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not attributed to the school or local authority
- security settings on personal social media profiles are regularly checked, to minimise risk of loss of personal information.

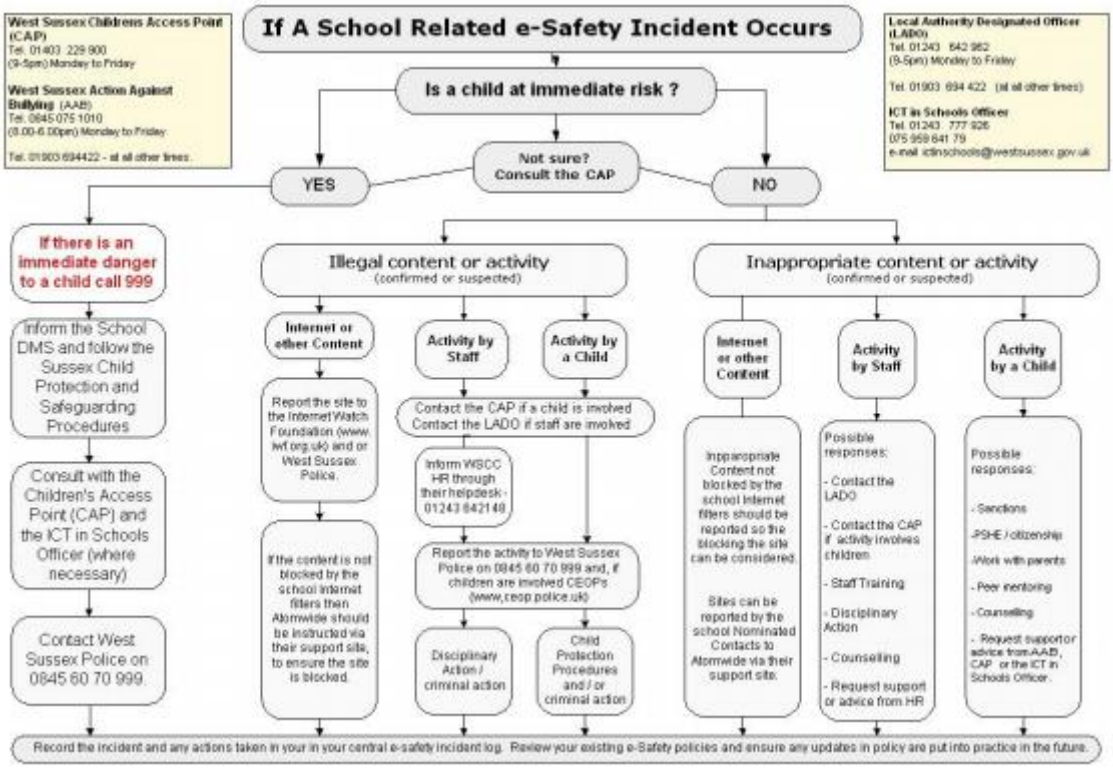
All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities and the appropriate action must be taken and recorded.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community, who understand and follow school policy, will be responsible users of digital technologies. However, there may be times when infringements of the policy could take place, through careless, irresponsible or deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the designated group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material

- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Responding to incidents of misuse

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Senior Leaders
- Computing Leader
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Pupils – Online Safety Group
- Parents / Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the FGB	Autumn 2017
The implementation of this Online Safety policy will be monitored by the:	Computing Leader & the Senior Leadership Team
Monitoring will take place at regular intervals:	Three times a year (termly)
The Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Three times a year (termly)
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2018
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	Local Authority Designated Officer (LADO) 03302 223339

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
- pupils
- parents / carers
- staff

Appendix A -
Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Computing Leader (or other relevant person, as above) with:

- the production/review/monitoring of the school Online Safety policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting parents/carers and the students/pupils about the Online Safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

(Appendix B - An Online Safety Group Terms of Reference)

Appendix B:
Filtering - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for Online Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the school's Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the school's Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by Surfprotect
- The school has provided enhanced / differentiated user-level filtering through the use of the Surfprotect filtering programme, allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the school's Network Manager and Computing Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through::

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the school's Network Manager and the Computing Leader who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person, the Computing Leader
- Online Safety Group
- Online Safety Governor
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Appendix C:
Online Safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The Online Safety committee will seek to include representation from all stakeholders.
The composition of the group should include:

- Middle Leadership Team member
- Teaching staff member
- Support staff member
- Online Safety & Computing Leader
- Governor
- ICT Network Manager
- Pupil representation – for advice and feedback. Pupil voice is essential in the makeup of the Online Safety committee, but pupils would only be expected to take part in committee meetings where deemed relevant.

2.2 Other people may be invited to attend the meetings, at the request of the Chairperson on behalf of the committee, to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve them or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed, they should be allowed to leave the meeting, with steps being made by other members to allow for these sensitivities.

3. DURATION OF MEETINGS

Meetings shall be held termly for a period of an hour. A special or extraordinary meeting may be called when and if deemed necessary.

4. FUNCTIONS

These are to assist the Online Safety Leader with the following;

- To keep up to date with new developments in the area of Online Safety
- To (at least) annually review and develop the Online Safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the Online Safety policy
- To monitor the log of reported Online Safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of Online Safety. This could be carried out through:
    - staff meetings
    - pupil forums (for advice and feedback)
    - governors meetings
    - surveys/questionnaires for pupils, parents/carers and staff
    - parents' evenings
    - website/VLE/Newsletters
    - Online Safety events
    - Internet Safety Day (annually - held on the second Tuesday in February)
    - To ensure that monitoring is carried out of Internet sites used across the school
    - To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
    - To monitor the safe use of data across the school
    - To monitor incidents involving cyberbullying for staff and pupils

5. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Waterfield Primary School have been agreed

Signed by (SLT):

Date:

Date for review:

Appendix D:
Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

School networked resources are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Conditions of Use

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Network Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school code of conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or the academy trust - TCT) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
3	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
4	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person. I will not reveal any of my personal information to students.
5	I will not trespass into other users' files or folders.
6	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
7	I will ensure that if I think someone has learned my password then I will change it immediately and contact the IT Network Manager.

8	I will ensure that I log off or out after my network session has finished or when I step away from the computer/laptop.
9	If I find an unattended machine logged on under another user's username I will **not** continue using the machine – I will log it off immediately.
10	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
11	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
12	I will not use the network in any way that would disrupt use of the network by others.
13	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the IT Network Manager.
14	I will not use "USB drives", portable hard-drives, memory sticks/cards or personal laptops on the network without having them "approved" by the school checked for viruses.
15	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
16	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
17	I will not accept invitations from children and young people to add me as a 'friend' to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my professional duties, such as school parents and their children.
18	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
19	I will ensure that the school's, and The Collegiate Trust's, names are not mentioned in any postings, status or images on social media sites that I contribute to.
20	I will support and promote the school's Online Safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates the Data Protection Act or breach security this act requires for personal data, including data held on Sims.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that all portable IT equipment such as laptops, iPads, digital still & video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

Additional guidelines

- Staff must comply with the acceptable use policy of any other networks that they access.
- Staff will follow the guidance provided by the e-PD on Online Safety - https://www.e-pd.org.uk/page/online-safety1
- Staff will follow the County Guidance on Staff Use of Mobile Phones in School.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the IT Network Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the IT Network Manager. Users identified as a security risk will be denied access to the network.

Media Publications

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

Further guidance can be found in the "Model Policy for schools regarding photographic images of children" August 2010.

Copies can be obtained from section 6 of the WSSS Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP

 -

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the IT Network Manager.

I agree to report any misuse of the network to the IT Network Manager.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the IT Network Manager.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the IT Network Manager.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: ____

Staff Signature: ______________________________

Date: _ _ /_ _ /_ _ _ _

Appendix E:
School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user can access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the school's IT Network Manager.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- Appropriate security measures will be in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the IT Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
- Users will be responsible for the security of their username and password, must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Computing Leader is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Mobile device security and management procedures are in place to ensure that the iPads and laptops are secured on the school's network through the Meraki system.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users.

- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site, unless passworded or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and the school's learning cloud, DB Primary.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "administrator" passwords for the school systems, used by the technical staff must also be available to the School Business Manager and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by the school's IT Network Manager.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.

Staff passwords:

- All staff users will be provided with a username and password by the school's IT Network Manager who will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- Must not include proper names or any other personal information about the user that might be known by others.
- The account should be "locked out" following six successive incorrect logon attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account login
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Should be changed at least every 60 to 90 days
- Should not re-used for 6 months and be significantly different from previous p the last four passwords cannot be re-used passwords created by the same user.
- Should be different for systems used inside and outside of school

Student / pupil passwords

- Pupils at EYFS and KS1 will receive a username and a 'picture password' in order to log onto the school's learning platform.
- Pupils at KS2 will receive a username and a password in order to log onto the school's learning platform.
- Students / pupils will be taught the importance of password security

- Pupils at EYFS and KS1 will receive a generic username and password to log onto the school's network system. For example; year 1 will log on as 'year1' and the password will be 'year1'. Towards the end of year 2, the children will be given their own individual usernames and passwords in order to log onto the school's network.
- Pupils at KS2 will receive their own individual username and password in order to log onto the school's network. In addition to this, the children will be able to log onto the network using a generic username and password. For example; year 3 will log on as 'year3' and the password will be 'year3'. This is to support the teacher and allow the children to work in groups/pairs whilst using the computer/IT equipment.

Parent passwords

- Parents of Waterfield Primary School, will receive a username and password to enable them to log onto the school learning platform. This will consist of an alpha-numeric password.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's Online Safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons through the Computing Online Safety curriculum
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person, IT Network Manager, will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Appendix F:
School Personal Data Handling Policy
Introduction
Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Policy Statements
The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data
The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities
The school's Senior Information Risk Officer (SIRO) is the Headteacher. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs), the School Business Manager, Computing Leader and the IT Technician for the various types *of* data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and

- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

Waterfield Primary School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Registration Number Z8820132 Expires: 30/11/2018