Alfred Street Junior School	Page 1 of 14
	Issued: October 2018
Online Safety Policy	Review date:
	Supersedes:
APPROVAL BY	FULL GOVERNING BODY /~~HEADTEACHER~~

This document has been produced with information given by The Key

Alfred Street Junior School believes that the use of information and communication technologies in schools brings fantastic benefits. However, recognising issues around online safety and planning accordingly will help ensure appropriate, effective and safer use of online technologies.

ICT and the internet have become integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world at the touch of a button.

Alfred Street Junior School is aware that children and staff cannot be completely protected from risk while using the internet. In accordance with Ofsted requirements, young people need to be empowered and educated in order to make healthy and responsible decisions when using the internet, now and in the future.

Members of staff are also aware and informed about how to manage their own professional reputation online, and demonstrate online behaviours that are in line with their role in school.

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on the school premises or on school devices.

The school will allocate internet access to staff and pupils on the basis for their educational need. Usage will be monitored and pupils will be aware that the school internet is filtered, with the understanding of the consequences of accessing inappropriate information.

The use of any computer system without permission, or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Northamptonshire Police.

This policy will be reviewed on a regular basis in line with any technological advances and developments.

Aims

Alfred Street Junior School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and prevent an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's Statutory Safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling online issues. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006, the Equality Act 2010 and the Education Act 2011.

This policy also takes into account the National Curriculum computing programs of study.

Roles and responsibilities

The governing board:

The governing board has overall responsibility for agreeing this policy as well as monitoring this policy, holding the Headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the ICT subject lead and the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see appendix 2)

The Headteacher:

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher / Senior Leaders are responsible for ensuring that the ICT subject lead and other relevant staff receive suitable CPD to enable them to carry out their online safety role and to train other colleagues, as relevant.

The designated safeguarding lead and ICT subject lead:

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy.

The DSL along with the ICT subject lead take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT subject leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

The ICT subject lead and external technicians

The ICT subject lead and external technicians are responsible for:

- Taking day to day responsibility for online safety issues and having a leading role in establishing and reviewing the school online safety policies / documents
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see appendix 2), and ensuring that pupils follow the school's terms on acceptable use (see appendix 1)
- Working with the DSL and ICT subject lead to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Staff will be given opportunities to discuss issues and develop appropriate teaching methods. If a member of staff is concerned about any aspect of their use of the internet on or off site they should discuss their concerns immediately with the Head Teacher or ICT subject lead.

Staff are fully aware of the importance of their online conduct in and out of school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Continue and implement online safety guidance at home with their families

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

And http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see appendix 2).

Educating pupils about online safety

Pupils will be taught about online safety in accordance with the 2014 National Curriculum requirements.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

All areas of online safety will be mapped out by the ICT subject lead for the teachers in relevant classes/year groups throughout the year to deliver the guidance essential for keeping children safe. These will be revisited regularly. If an incident arises during the year, additional sessions will be delivered to the relevant classes/year groups.

Online safety should be a continuing focus in all areas of the curriculum and staff should reinforce online safety messages, wherever possible, in the use of computing across the curriculum.

Where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use. Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit, thus encouraging responsible use. Child friendly search engine examples can be found on the online safety display in the computing suite.

It is accepted that from time to time, for good educational reasons, pupils 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 external technician can temporarily remove those sites from the filtered list for the period of study. Any request should also be brought to the attention of the Headteacher and ICT subject lead with clear reasons provided.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The pupils will sign the acceptable use policy (see appendix 1)

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website social media page. This policy will also be shared with parents.

The school will make use of and cascade useful online safety resources out to the parent and the school community.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher/the DSL and/or the ICT subject lead.

Use of digital and video images

When using images and video, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, publishing and distributing of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

Staff 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, under no circumstances should the personal equipment of staff be used for such purposes.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school's home school agreement (which seeks parental consent) on the use of images. An updated list will be kept by the school office and this list will also be given to all staff. Pupils' full names will not be used anywhere on a website or online document, particularly in association with photographs.

Communication technologies

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Headteacher or ICT subject lead – in accordance with the school policy, the receipt of any email that makes them feel

uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and students / pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils at KS2 will be provided with individual school email addresses for educational use (when and if appropriate)
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Cyber-bullying

Definition:

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying:

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health education (PSHE), and other subjects where appropriate.

The school may also send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material

has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in liaise with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (weekly) to ensure they comply with the above. Relevant and appropriate action will be taken if inappropriate websites are accessed.

Rules for use of school devices and the internet will be discussed with pupils. These will be posted in classrooms and displayed on the online safety display board in the computer suite.

More information is set out in the acceptable use agreements (see appendices 1 and 2).

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. They must hand them into the office in the morning and collect them after school. Parents must sign a consent form before pupils can bring mobile devices to school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use (see appendix 2).

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted/password protected.

If staff have any concerns over the security of their device, they must seek advice from the ICT subject lead or the external technicians.

Work devices must be used solely for work activities and may not be used by family members unless supervised.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, newsletters and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring arrangements

All staff will log behaviour and safeguarding issues related to online safety (see appendix 3). This policy will be reviewed annually by the ICT subject lead. At every review, the policy will be shared with the governing board for final approval.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy
- Complaints procedure

Appendix 1: Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I WILL NOT:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the school day, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- I will hand it into the school office at the beginning of the day and collect it at the end of the day.

I agree that the school will monitor the websites I visit.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites (unless for school purposes) or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
I agree that the school will monitor the websites I visit.
I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
I will let the designated safeguarding lead (DSL) and ICT know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date:

Appendix 3: Online safety incident report log

Date	Description of the incident (Who, where, what and when)	Action taken	Name of staff member recording the incident
