Arbour House School

Online Safety Policy

Policy Number	16
Date of Issue	February 2022
Version number and validation date	V4 - September 2024
Next review date	September 2025
Governor policy owner	Charlie Smith
Signed off by	Arbour House School Governing Body
Distributed to	Internal/ External

Introduction

This policy applies to all members of the Arbour House School community - staff, pupils, volunteers, parents/carers and visitors - 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 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 hours, 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.

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.

Board of 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 receiving regular information about online safety incidents and monitoring reports.

The Board of Governors must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

The Board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

A member of the Governing Body (currently Bettina Jeppesen, Potens Operations Director, South) has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include oversight of the above which will require:

- Regular meetings with the school's Online Safety Champion and/or DSL
- Regular monitoring of any online safety incidents or concerns

- Regular monitoring of filtering/change control logs
- Reporting any issues or concerns to the Headteacher, other Governors where relevant and to the Board of Proprietors.

Headteacher

The Headteacher has a duty of care for ensuring the safety, including online safety, of members of the school community, although the day-to-day responsibility for online safety will be delegated to the Online Safety Champion.

The Headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. *(See Appendix 1: 'Flow Chart on Dealing with Online Safety Incidents' and 'Responding to Incidents of Misuse')*

The Headteacher is responsible for ensuring that the Online Safety Champion and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher 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 support to those colleagues who take on important monitoring roles.

Online Safety Champion:

- 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.
- Co-ordinates training and advice for staff
- Liaises with the Local Authority/LADO/relevant body
- Liaises with school technical staff
- Receives reports of online safety incidents (via 'Cause for Concern') and creates a log of incidents to inform future online safety developments.
- Reports to the Online Safety Governor to discuss current issues, review incidents or concerns and filtering/change control logs.
- Reports regularly to the Headteacher/DSL.

Technical ICT Staff (this function is carried out by Potens' IT Department through WorkplaceIT):

Technical ICT Staff are 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 or other relevant body Online Safety Policy or 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 arrangements are applied and updated on a regular basis and their implementation is not the sole responsibility of any single person
- 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Coordinator / for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy/ Agreement (AUP) (Appendix 4)
- They report any suspected misuse or problem to the Headteacher and Online Safety Champion for investigation/action /sanction
- All digital communications with 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
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils are taught about research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned 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

Designated Safeguarding Lead (DSL):

At Arbour House School the overall DSL is the Headteacher. The Deputy Headteacher, Head of Lower School and the Head of Upper school also act as DSLs. The DSLs are trained in Online Safety issues and are 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
- cyber-bullying

They will also take the lead on understanding the filtering and monitoring systems that we have in place through the Smoothwall proramme

and processes in place on school devices and school networks.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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
- 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 community.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through discussion with school staff, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the 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 website
- Their children's personal devices in the school

Education and Support for 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:

1. A planned online safety curriculum will be provided as part of ICT/RSHE/PSHE/ ILS and other lessons and should be regularly revisited.
2. Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
3. Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

4. Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
5. Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. This takes account of additional duties for schools under the 'Counter Terrorism and Securities Act 2015' which requires schools to ensure that children are safe from terrorist and extremist material on the internet. All staff complete the government PREVENT training.
6. Pupils will be helped to understand the need for the 'Pupil Acceptable Use Agreement' and encouraged to adopt safe and responsible use of ICT both within and outside school.
7. Pupils will be taught to understand the benefits of AI and also that it has the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.
8. Pupils will be made aware that the school will treat any use of AI to bully pupils in line with our Anti-Bullying Policy.
9. Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
10. In lessons where internet use is pre-planned, it is best practice that 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.
11. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and not leave pupils unsupervised for any duration of time.
12. Anything that pupils search for on the internet, that is inappropriate, will be identified by our filtering and monitoring system and the appropriate staff will be alerted to its use.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics e.g. 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 set period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education and Support for Parents/Carers:

Many parents/carers have 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 their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure how to respond.

The school will therefore seek to provide information and raise awareness to parents/carers through:

- Offering training for parent/carers via the Online Safety Alliance.
- Curriculum activities
- Letters and information sent home

- ‘Staying Safe’ section on the school website that includes Online Safety
- Discussion with teachers and school staff
- Reminders about high profile events/campaigns e.g. Safer Internet Day
- Raising awareness of useful websites and sources of further support e.g. www.saferinternet.org.uk and www.childnet.com/parents-and-carers

(See appendix for further links/resources)

Training for Staff

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:

- Formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training of all staff will be carried out regularly and a record kept of when Online Safety training is due for renewal.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school’s Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process or through their Line Management procedures.

The Online Safety Champion will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

The Online Safety Champion will ensure that all staff and parents/carers receive any information deemed necessary to ensure the safety of our pupils.

This Online Safety Policy and its updates will be presented to staff who will sign to say they have read and understand it.

Training for Governors

Governors should take part in Online Safety training, with particular importance for those who are members of any group involved in monitoring Online Safety, Health and Safety and Safeguarding at the school.

Governor Training may be accessed via

- Attendance at training events provided by the Local Authority, National Governors Association, or other relevant organisation (e.g. SWGfL).
- Participation in school information sessions for staff or parents

Technical – Infrastructure/Equipment, Filtering and Monitoring

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.

The school will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. This is done through the Smoothwall proramme.
- All school devices will be monitored through the Smoohtwall programme and staff will be alerted via email when there are safety breaches that need addressing
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All staff will be provided with a username and secure password by the IT team. Users are responsible for the security of their username and password *and will be* required to change their password every term.
- The IT Department 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.
- Internet access is filtered for all users through the Smoothwall proramme. 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 for more details).
- Internet filtering ensures that children are safer from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users – staff/pupils.
- The Smoothwall programme monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement (Refer to Appendices).
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- 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. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

- Staff and pupils are forbidden from downloading executable files and installing programmes on school devices. The complexities around certain programmes not being filtered are monitored by the IT Department.
- An agreed policy is in place regarding the use of removable media (e.g. 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 (*see* the Information and Data Governance, Protection and Management Policy for further detail).

Mobile Technologies

Mobile technology devices used at school and off-site for the purposes of school-related work will be school owned and might include smartphone, tablet, notebook/laptop, or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of school-owned mobile technology devices is educational only.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, parents/carers and pupils 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 pupils 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.
- Unless we receive written permission from parents/carers photographs/videos/ audio of pupils will not be published on the school website, on social media, in the local press or for promotional purposes. Only pupils' first names will be included, surnames will not be used without permission.
- In accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images of their children at school events for their own personal use. At Arbour House however we ask that

parent/carers do not do so in the best interest of our pupils, many of whom suffer with anxiety and would find such 'intrusion' distressing and confusing
- 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, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the school website, or elsewhere that includes pupils 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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

The School details general data protection in its policy **Information and Data Governance, Protection and Management** and staff must ensure they are familiar with this.

Staff must ensure that they:

- At all times take care to ensure the safe keeping 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.

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

- the data must be encrypted, and 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 (below) once it has been transferred or its use is complete

The Information and Data Governance, Protection and Management Policy provides more detailed guidance on the school's responsibilities and on good practice.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The benefit of using these technologies for education outweighs the risks. The learning of the pupils will determine the technologies and their use.

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 should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the nominated person 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.
- Any digital communication between staff and pupils or parents/carers should be via school email only and must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- 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 email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Schools 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 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:

- Ensuring that personal information is not published.
- Training is provided including acceptable use; social media risks; checking of settings; data protection; 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 pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used it should not associate itself with the school or impact on the school.
- Where excessive personal use of social media in school time is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Links to Other School Policies:

Safeguarding & Child Protection Policy

Health and Safety Policy

Appendices:

1. Responding to Incidents of Misuse - Online Safety Incident Flow Chart
2. Pupil Acceptable Use Agreement
3. Parent/Carer Acceptable Use Agreement/Permission
4. Staff Acceptable Use Agreement
5. Links to Other Organisations and Documents for Information or Support

Appendix 1: Online Safety Incident Flowchart

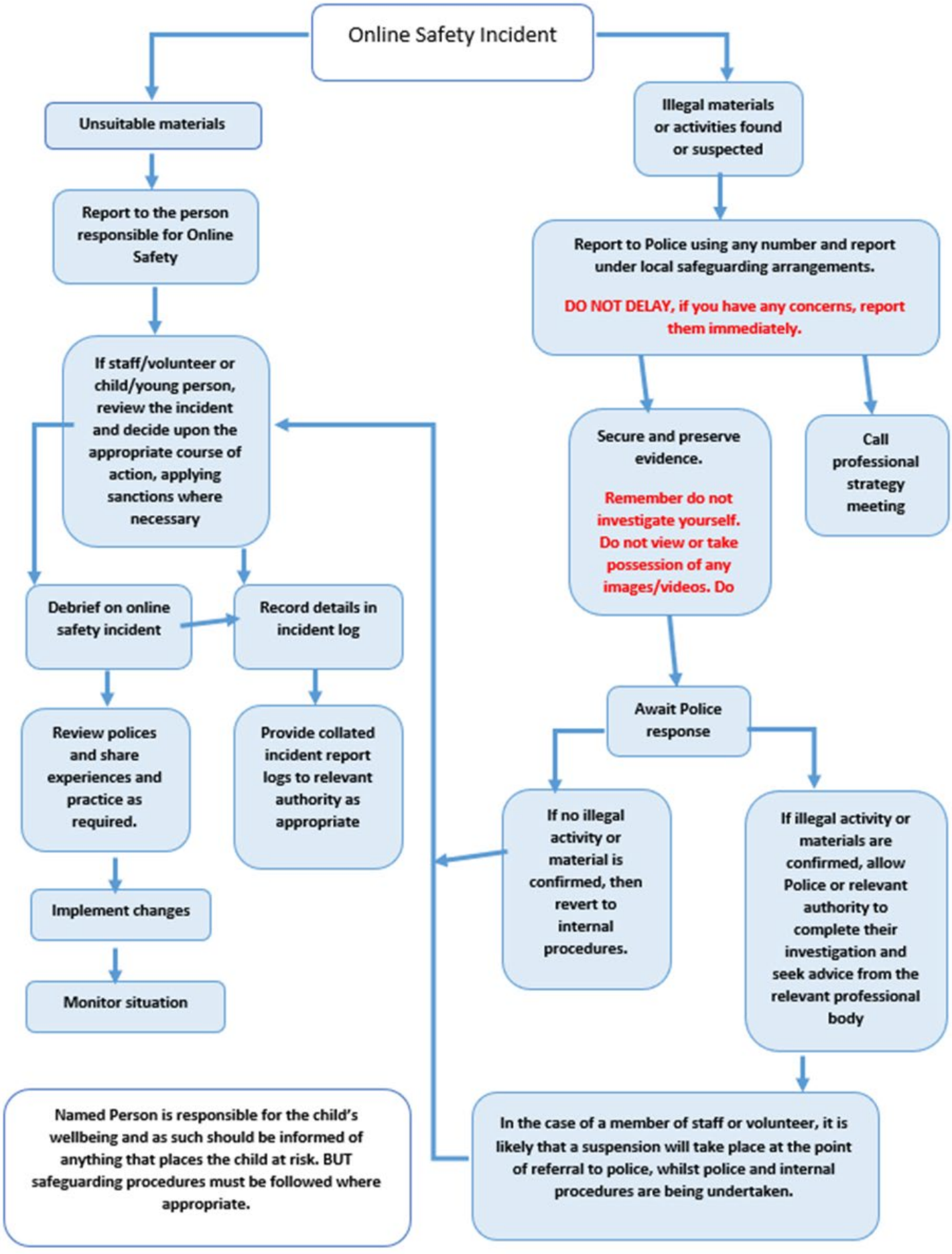
Responding to Incidents of Misuse

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.

Illegal Incidents

If there is any suspicion that the website(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 and appendix) for responding to online safety incidents and report immediately to the police.

Online Safety Incident Flow Chart



Appendix 2

Pupil Acceptable Use Agreement for Online Safety and Use of Digital Technologies in School

Below is the agreement that all pupils will have read and explained to them by school staff. They will be required to sign a copy and this signed copy will be kept in their secure Pupil File. This document is also given to all parents/carers so they know what their child has been asked to sign and so they can support their child's understanding of acceptable use of digital technologies in school.

Arbour House School Rules for Responsible Computer and Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others whilst using the school computer system with the permission of staff.

- I will use only my own login and password;
- I will not access other people's files;
- I will only use the computers when I have permission from a member of staff;
- I will not bring stored files into school without permission;
- I will ask permission from a member of staff before using the Internet;
- I will not use the Internet unless supervised by a member of staff;
- I will not create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- I will only e-mail people that a teacher or member of school staff has approved;
- The messages I send will be polite and sensible;
- I will not give out my personal information (for example my age, surname, address, school, email or phone number)
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or if I receive a message I do not like;
- I understand that the school can check my computer files, my emails and the Internet sites I visit.

Rules for bringing a digital device to school

I understand that I must hand any electronic device, including mobile phones to the School Office. They will be kept safe and secure. I cannot use it in school time. If I don't follow the rules the device will be taken off me until the end of the day. If this happens more than once, the device will only be returned when my parent/carer collects it from the School Office. I may not be allowed to bring a device into school from then on.

Pupil Agreement:

I agree to follow the 'Rules for Responsible Computer and Internet Use' and to the 'Rules for bringing an electronic device to school'.

Signed: ... ...

Print name: ... ...

Class: ... ...

Parent/Carer's Permission & Agreement:

I give permission for my child's access to the Arbour House School computer network, including the Internet on the terms set out in the above rules. I also agree to the rules set out for use of personal digital devices in school.

Signed: ... ... Print name: ... ... Date: ... ...

Appendix 3

Parent/Carer Acceptable Use Agreement for Online Safety and Use of Digital Technologies in School

Below is the agreement that is given to all parents/carers.

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people regarding their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the 'Pupil Acceptable Use Policy' is attached to this permission form, so that parents/carers will be aware of the school's expectations of the young people in their care.

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

Parent/Carer Permission Form

As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to ICT systems at school.

I understand that the school has discussed the 'Pupil Acceptable Use Agreement' with my child and that they will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

I will support the school in the rules around bringing a digital device to school, including the use of phones. I understand that if the rules are not followed the device will be taken off the child until the end of the day. If this happens more than once, the device will only be returned when I collect it and my child may then not be allowed to take a device to school from then on.

I understand that the school will take no responsibility for lost, stolen or damaged devices which are brought into school.

In addition to the above as a parent/carer I will act responsibly when using internet, mobile technologies and social media in relation to the school or members of the school community.

I understand that if I take any digital images of my child, they will not include any other pupils from Arbour House School.

Parent/Carer's Name: .....

Pupil Name: .....

Signed: .....

Date: .....

Appendix 4

Staff Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and raise awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff will have good access to digital technology to enhance their work, and to enhance learning opportunities for pupils' learning and in return the school expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use school mobile devices I will follow the rules set out in this agreement.
- I will also follow any additional rules set by the school about such use.
- I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure my data is backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent others from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Information and Data Governance, Protection and Management Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the Information and Data Governance, Protection and Management Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any loss, damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (when carrying out communications related to the school or about the school) within these guidelines.

Staff Name: .....

Signed: .....

Date: .....

Appendix 5

Links to Other Organisations and Documents for Information or Support

Safer Internet Centre – http://saferinternet.org.uk/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Internet Watch Foundation - https://www.iwf.org.uk/

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - http://www.netsmartz.org/

Respectme - http://www.respectme.org.uk/

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Facebook Guide for Educators

For Parent and Carers:

Connectsafely Parents Guide to Facebook
Online Safety BOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

POLICY REVIEW RECORD

POLICY NAME	**Online Safety Policy**	
COMPILED BY	Charlie Smith	
DATE	February 2022	
REVIEW DUE DATE	**REVIEWED**	
	DATE	**BY Name & Amendments Made:**
September 2023	Sept 2023	Julie Perks: added in line with DfE Statutory Guidance ***Roles and Responsibilities*** <u>*Designated Safeguarding Leads (DSLs):*</u> *They will also take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.*
		Roles and Responsibilities <u>*Board of Governors*</u> *The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:* • *Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;* • *Reviewing filtering and monitoring provisions at least annually;* • *Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;* • *Having effective monitoring strategies in place that meet their safeguarding needs.* **Education and Support for Pupils** • Pupils will be taught to have an understanding of the benefits of AI and also that it has the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. • Pupils will be made aware that the school will treat any use of AI to bully pupils in line with our anti bullying policy.

	Oct 2023	Charlie Smith added to: • Appendix 2: The pupil acceptable use agreement, now has the addition: *"I will not create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate."*
September 2024	Sept 2024	Julie Perks added the OSA as a source of training for parent/carers.
	Jan 2025	Charlie Smith added details around the Smoothwall monitoring and filtering system that the school has in place.