Online Safety / Acceptable Use Policy (AUP)

Autumn 2020
Review: Autumn 2023

Writing and reviewing the AUP

The AUP is part of the School Development Plan and relates to other policies including those for ICT, bullying and child protection.

- **The school will appoint an Online Safety coordinator. In many cases this will be the Designated Safeguarding Lead as the roles overlap. Waverley Abbey' s Online Safety coordinator is Ms D Morris.**
- Our AUP has been written by the school, building on best practice and government guidance. It has been agreed by Senior Leadership Team and the Local Governing Committee.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access is provided by Surrey's recommended supplier "UNICORN" and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable, what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to get themselves out of bad situations or report unpleasant Internet content e.g. using the **thinkuknow** website and the CEOP Report Abuse icon.
- Pupils will be encouraged to report anything which they encounter on the internet which makes them feel uncomfortable; they will not be blamed for accidental or inadvertent incidents.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly, by the Network Manager, reporting to the SLT.
- Virus protection is updated daily.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Only school devices Desktops, Laptops, Learnpads and Smartphones may have access to the School's Wi-Fi..

E-mail

- **Pupils and staff may only use approved e-mail accounts on the school system.**
- Pupils will not be issued with individual school email accounts.
- Pupils will be instructed to immediately tell a trusted adult if they receive offensive e-mail, whether during email lessons in school or on a home email account.
- Pupils will be instructed not reveal personal details of themselves or others in e-mails or arrange to meet anyone without specific permission, within school or at home.
- Staff to pupil email communication, when and if necessary in particular circumstances, must only take place via a school email address
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff, pupils or Local Governing Committee (LGC) members' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate and monitored each half term.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents and Local Governing Committee members will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with The Good Shepherd Trust to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and the ICT Network Manager.
- The ICT Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

All personal data is recorded, processed, transferred and made available according the General Data Protection Regulation (GDPR).

- **The First Principle - Lawfulness, fairness and transparency**
  Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)].

- **The Second Principle - Purpose limitations**
  Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

- **The Third Principle - Data minimisation**
  Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing**.**

- **The Fourth Principle – Accuracy**
  Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

- **The Fifth Principle - Storage limitations**
  Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. In summary, data no longer required should be removed.

- **The Sixth Principle - Integrity and confidentiality**
  Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)].

These 6 principles give a top level overview of the areas covered by the new regulation, however they do not delve into nuances of consent and other articles of GDPR, nor the complexities of data flow mapping, lineage and coordination activities associated with implementing a program to meet GDPR compliance.

The Diocesan GDPR Policy can be found here https://www.cofeguildford.org.uk/about/data-policies

The school is registered with the Information Commissioner's Office (ICO) under The Good Shepherd Trust's registration. All members of staff will be made aware of the data protection principles when processing personal data. This is covered in staff induction and at other appropriate training sessions.

Policy Decisions

Authorising Internet access

- All staff and members of the LGC must read and sign the 'Staff Code of Conduct' (for IT) before using any school ICT resource [See Appendix A].
- The School's internet filtering systems and 'Responsible use of ICT – Rules for e-Safety'[see Appendix B] will be explained to parents. Parents will be informed that their consent for their child to access and use the internet in school is assumed; parents may withdraw this consent by writing to the school, though it will be explained that their child may view websites as part of whole class or whole school activities.
- All pupils must have the 'Responsible use of ICT Rules for e-Safety' explained to them by their teacher [see Appendix B] Parents are encouraged to discuss the e-Safety rules with their child(ren).
- Any person not directly employed by the school (including volunteers) will be asked to sign an 'Acceptable use of school ICT resources' before being allowed to access the internet from the school site (see Appendix D).

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than close-up photos of individual children. Inappropriate photographs will not be published.
- Pupils' full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums or wikis; full names will not appear alongside photographs.
- Parental consent for publication of their child's photographs is requested when the child joins the school for the following platforms
    - School Website
    - Facebook
    - External Publications (including but not limited to) Local Newspapers, Village/Parish Magazines
- Parents should be clearly informed of the school policy, which is on the school website, on image taking and publishing, both on school and independent electronic repositories.
- Twitter is not actively used. It is connected to Facebook for updates but will only add the first few lines of any Facebook post.

Publishing Staff and members of the LGC's details

- No personal details relating to staff will be published online by the School, apart from their names and professional roles in relation to the school.
- No personal details relating to members of the LGC will be published online by the School, apart from the information required by the Academies financial handbook and Get Information About Schools (GIAS).
- Photographs of staff and members of the LGC will only be published on the School's website, Facebook or External Publications with their permission.

Use of mobile communication and internet technologies

- Staff will not contact a pupil direct outside of school by 'phone or email; contact will always be made via the pupil's parent, carer or guardian.
- The school has a range of mobile digital devices available to staff for use in teaching and learning. `
- Staff will not use mobile phones, devices or cameras **for their own personal use** when they are on duty.
- No photographs of any children are to be taken on Staff's personal devices.
- If any a member of staff wishes to use other devices e.g. belonging to staff or pupils for teaching and learning then this must be discussed and agreed with the SLT prior to their use and appropriate online safety procedures established and followed. It must be ensured that pupils are not able to access inappropriate content or store photographic or other data of pupils on their personal devices.
- Other devices such as tablets and e-readers that have Internet access but may not include filtering and must be approved for use by the ICT Department before use.
- Any device not issued by the School must be assessed by either the school's ICT Technician or Network Manager to ensure the safety of the school's network before any network connection is attempted.
- Care will be taken with use of such devices within the school where an educational benefit is identified for their use.
- The sending of abusive or inappropriate text messages is forbidden.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the AUP is adequate and that the implementation of the AUP is appropriate and effective.
- Monitoring software will be used to ensure appropriate staff and pupil conduct when using ICT in school. Instances of potential inappropriate behaviour thus reported will be raised with the appropriate member of staff, Online Safety Coordinator or SLT.
- Where a member of staff wishes to use a blocked website within school, he/she shall explain their reasons to their Year Leader and then, if agreed, request permission for the site to be unblocked from the Senior Leadership Team.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Sanctions for breaches of the AUP

- Instances where a pupil deliberately breaches the AUP will be dealt with by the Class Teacher, Year Leader or Headteacher according to the nature and severity of the breach. Emphasis will be on educating the pupil in online safety. Where appropriate the parents/carer of the pupil will be informed; the pupil may be prevented from using ICT or the internet within school for a period of time.
- The Headteacher will deal with instances where a member of staff has breached the AUP. Depending on the severity of the breach disciplinary procedures may be invoked.
- Breaches of the AUP by a member of the LGC or Headteacher will be referred to the Good Shepherd Trust immediately.

- The Headteacher or Chair of the LGC will follow the GST advice when dealing with breaches of the AUP by members of the wider school community; access to the school's information systems may be withdrawn from the individual.

Communication of the Policy

Introducing the AUP to pupils

- Appropriate elements of the AUP will be shared with pupils
- Online Safety rules will be posted in all networked rooms.
- The Online Safety rules will be explained to the pupils during specific Computing lessons at the beginning of each academic year and reinforced whenever the internet is used within lessons. Pupils will be encouraged to report anything that they are uncomfortable about that they come across on the internet; they will be assured that such inadvertent instances are not their fault.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be involved in the review of the AUP; their views on Online Safety and suggestions will be actively sought and encouraged.

Staff and the AUP

- All staff will be given the School AUP and its importance explained. All staff will be required to sign the Code of Conduct.
- The views of staff will be sought during the review of the AUP.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- **Staff that manage filtering systems or monitor ICT use will be supervised by Senior Leadership and have clear procedures for reporting issues.**

LGC members and the AUP

- All members of the LGC will be given the School AUP and its importance explained. All members of the LGC will be required to sign the Code of Conduct.
- Staff and members of the LGC should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School AUP in newsletters and on the school web site.
- Parents and carers will from time to time be provided with additional information on e-safety. Their views will be sought during the review of the AUP.
- The school will inform all new parents of the School's AUP and the assumed consent for pupil internet use when they register their child with the school.

Appendix A Staff and Local Governing Committee Code of Conduct for ICT

Waverley Abbey C of E Junior School

Staff and Local Governing Committee Code of Conduct for ICT

To ensure that members of staff and members of the LGC are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. The school's Online Safety Policy and/or Online Safety Coordinator should be consulted for further information or clarification.

- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or LGC.
- I will ensure that all electronic communications with pupils, parents, staff and members of the LGB are compatible with my professional role.
- Images of pupils and/ or staff / members of the LGC will only be taken, stored and used for professional purposes in line with this school policy. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff, / Headteacher or member of the LGC.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will comply with the school's ICT system security and not disclose any school related passwords.
- I will only use the approved, secure email system(s) for school business only.
- I will ensure that personal data (such as data held on Pupil Asset is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I understand that personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or LGB.
- I will not install any hardware or software on school systems without permission.
- I will respect copyright and intellectual property rights.
- I will not use mobile phones, mobile devices, cameras or other technology for personal use when I am on duty.
- I will ensure that any mobile digital devices used within school are approved for such use. I understand that all my use of the Internet and other related technologies may be monitored and logged and can be made available, on request, to my Line Manager, Headteacher and the LGB and GST trust board.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

I [give] / [do not give] permission for my photograph to be published on the school's website.

Signature …… **Date** ……

Full Name ……..(**printed**)

Job title / role . ……

Return one copy to the school office; retain the other copy for your records. *Autumn 2020*

Appendix B Pupils' Responsible use of ICT Rules for Online Safety'

We use the School's computers, tablets and the internet for learning.
These rules will help us to be fair to others and keep everyone safe.

Responsible Use of Technology

I will always use technology in school responsibly:

- I will only open, update and delete my own or shared files, and I will keep my passwords safe.
- I will ask permission before going to a website or using files from memory devices e.g. DVDs, memory sticks.
- I will not deliberately type, send or search for anything that could be unpleasant, rude or nasty.
- I will use equipment with care and report any problems immediately.
- All online contact I make with other children and adults, inside and outside of school, will be polite and sensible.

Rules for Online Safety

The internet can be a fun and great way to chat, share files and listen to music.
*But remember, **once you have sent text, photos or videos you lose control** – it can be sent to anyone: teachers, parents, grandparents, anyone and everyone. So, …*

be SMART and stay safe, in school & at home

S AFE	I will not give my full name, address, phone number, email address, photos or school name.
M EETING	I will not arrange to meet someone I have met online.
A CCEPTING	I will ask for permission before opening an online message sent by someone I do not know.
R ELIABLE	I understand that not everything on the internet is true and people may not be who they say they are.
T ELL	If something makes me uncomfortable or worried, or someone asks for my personal details, I will tell an adult I trust.

- ✦ I know that my use of computers in school can be checked and my parent/carer will be contacted if a member of the school staff is concerned about my e-safety.
- ✦ I understand that if I deliberately break these rules, I could be stopped from using the internet or computer technology in school.

Name: …… Class: ……

Signed: …… Date: ……

Appendix C Acceptable Use of ICT – Wider community

Waverley Abbey C of E Junior School

Acceptable Use of school ICT resources by members of the wider school community

(excluding, staff, members of the LGC and pupils)

To ensure that members of the wider school community are aware of Online Safety and their responsibilities when using the school's ICT systems, they are asked to sign this code of conduct.
The school's Online Safety Policy should be consulted for further information or clarification.

- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will only use the school's email / Internet / Intranet and any related technologies for purposes deemed reasonable by the Head Teacher, or governing Committee or their delegated representatives.
- Images of pupils and/ or staff will only be taken, stored and used for purposes in line with school policy. Images will not be distributed outside the school network or social media without the permission of the parent/ carer, member of staff or Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use mobile phones, mobile devices, cameras or other technology for personal use whilst I am in School.
- I will ensure that any mobile digital devices used within school are approved for such use.
- I will ensure that my online activity in school will not bring the school into disrepute.
- I will comply with the school's ICT system security and not disclose any school related passwords.
- I will not install any hardware or software on school systems.
- I will respect copyright and intellectual property rights.

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

I require access to the school's information systems for:
……..……..(*please give the reason*)

during the period: ……..……*ease give dates/time*)

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …….…… **Date** ……..……

Full Name ……..…….(**printed**)

Staff authorisation : ……(**signed**) ……(**name**)

Return one copy to the school office; retain the other copy for your records. *Autumn 2020*

OFFICE USE: Username created/allocated: