Oldbury Wells School
Digital & E-Safety Policy
2023-24

FREQUENCY OF REVIEW:	Annually
RATIFICATION DATE:	Autumn Term 2023
RATIFIED BY:	OWS Local Governing Body
DATE OF NEXT REVIEW:	September 2024
AUTHOR:	Deputy Headteacher (TZW)

Adopted by the Oldbury Wells School Local Governing Body

Signed: _____ Chair of LGB   Date: _____

Signed: _____ Headteacher   Date: _____

Contents   Page

Responsibilities

The members of staff responsible for e-safety and digital technologies are:

Mr Tom Williams - Deputy Headteacher

Mrs Joanne Green - Safeguarding Officer

The Governor responsible for e-safety is: Connor Robinson

The e-Safety Co-ordinator is: Tom Williams

The e-Safety Co-ordinator is responsible for leading the e-Safety Committee, delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the school community. They may also be required to deliver workshops for parents.

Oldbury Wells School is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective way to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure and the safety of its users is the responsibility of all staff.

e-Safety Co-ordinator

The school e-Safety Co-ordinator is responsible for e-safety. They will meet with representatives from the following groups: SLT, governors, teaching staff and the ICT Network Manager to discuss issues surrounding e-safety. Any issues will be fed back to the Governors.

Governors/Board of Directors

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. A member of the *Governing Body/Board* has been assigned as a link governor for e-safety & digital technologies. The role of the link governor will include:

- meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting.

Headteacher/Principal and Senior Leaders

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.

- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (These are outlined in the schools disciplinary and safeguarding policies)

- *The Headteacher/Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead 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/Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.*
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Online Safety Lead

- leads the Online Safety Group.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority/MAT/relevant body.
- liaises with school technical staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety *Governor and network manager* to discuss current issues, review incident logs and filtering/change control logs.
- attends relevant meetings of *Governors/Directors.*
- reports regularly to Senior Leadership Team.

Network Manager/Technical Staff

The school has a managed service by Telford & Wrekin IT Services. Those with technical responsibilities 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/MAT/other relevant body* online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- *the filtering policy is applied and updated on a regular basis and that its 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 *networks/internet/digital technologies* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Headteacher and Senior Leaders* 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/AUA)
- they report any suspected misuse or problem to the *Headteacher/Principal/Senior Leader/Online Safety Lead* for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/pupils have a good understanding of 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 with regard to these devices
- *in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that if any unsuitable material that is found in internet searches the network manager is informed.*

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

Online Safety Group

This is comprised of:

- Deputy Headteacher with responsibility for ICT
- Designated safeguarding lead
- Head of IT
- Network Manager

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

- the production/review/monitoring of the school online safety policy/documents.
- *the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.*

- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions.

Students/Pupils:

- are responsible for using the *school* digital technology systems in accordance with the student/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 online-bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* online safety policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media 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/Learning Platform and on-line student/pupil records *their children's personal devices in the school (where this is allowed)*

To support this the school will use half termly e-safety updates to make parents aware.

Acceptable Use Policies (AUPs)

This acceptable use policy relates to any ICT use in school or on school business. It relates to all school equipment and all school initiated communication systems - this includes all work within the cloud. As such the policy provides guidance for our working and private practice both within and outside of school. In particular this policy extends to out of school use including:

- Our email system from any location
- Use of school equipment in and out of school
- The access to the school's Office 365 applications via the internet and Microsoft Teams and Show My Homework.

You must be aware that any infringement of current legislation, ie Data Protection Act 1998 and General Data Protection Regulations (GDPR), Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988, will be regarded as a breach of school policy and may be treated as gross misconduct. In some circumstances such a breach may also be a criminal offence.

ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and, as such, **all** users have a personal responsibility for ICT security and safety both inside and outside of school.

All members of the school community should agree to an Acceptable Use Policy (AUP) that is appropriate to their age and role. AUPs used can be found in **Appendix 1.**

A copy of the pupil AUP will be signed as part of the school registration form. This can be found in **Appendix 1.**

AUPs will be reviewed periodically. All AUPs will be stored centrally in case of breaches of the e-safety policy.

E-safety forms a part of all IT teaching and the AUP will form part of this.

Internet Use

All internet activity should be appropriate to the function of educating, or supporting the education of children, young people and adult learners in school related matters.

All staff and pupil internet usage is monitored through SENSO. This is monitored weekly, logged and kept for an appropriate length of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are only available to authorised personnel and kept for no longer than necessary in line with the current data protection policy.

The use of public chat rooms and social media sites/applications is not allowed on school equipment or via Personal Electronic Devices (PEDs) whilst on the premises. However, professional on-line forum may be appropriately used for professional business and/or professional development. Posting anonymous messages and forwarding chain letters is forbidden. Comments or information which harms the school or school members may not be posted or distributed.

Photographs and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet.

- When using digital images, staff should inform and educate students/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.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press:

  - Under GDPR regulations photos are classed as personal data. As a school we must have a lawful basis to use these. In most cases this is part of our public task of

education e.g. photos/videos needed for exam courses or to support teaching and learning.
- However, where photos are required for other purposes (e.g. school marketing) consent is the other lawful basis that can be used. When this is the case and in using all photos pupil records should be checked. (This data is held in SIMS).
- Staff must be fully aware of the consent form responses from parents when considering use of images. The consent form is part of the school registration form and all data can be accessed in SIMS **(Appendix 2).**

It is the member of staff's responsibility to ensure that this is checked at the point of taking the photo and before uploading any media to the school website. The schools will review these permissions annually.

Photos and Videos taken by Parents/Carers

Parents and carers are not permitted to take photos/videos of children in school events unless they are given specific instructions from a member of the SLT. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. In the rare event that this takes place them they should be removed from devices and uploaded onto the school system within 48 hours.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

With any displays of personal information safeguarding risks should be evaluated as well.

Mobile phones and other Personal Electronic Devices (PEDs)

Pupils and staff mobile phones should be switched to silent whilst on the school premises and remain out of sight and not used. Pupil phones and PEDs found to contravene this should be confiscated in line with the school's behaviour policy.

There may be times when some of the features of mobile phones or PEDs may be beneficial to the learning activities in a lesson (eg pupils may wish to capture photos/videos of an experiment). In such cases mobile devices can be used once permission has been granted by the teacher – this should only occur when it promotes good standards of teaching and learning.

If a member of staff suspects a mobile phone or PED has been misused or is used in a manner not specified by the class teacher (e.g. taking a photograph of another student), the mobile phone or PED may be confiscated. A senior member of staff my seek permission to search the mobile phone or PED.

Mobile phones and PEDs should only be used to access the internet when specified by members of staff, using the school's internet connection. Use of personal 3G/4G connections (or other data connection) should only be used under specific direction of a member of staff, as should using the mobile phone or PED for any form of communication during the school day or during school activities.

Visitors to school should ensure that mobile phones are switched off and not used on the school site.

Appendix 4 provides a guide for the use of mobile technology within school.

Security and Passwords

Staff are informed that they must change passwords regularly. Best practice indicates that passwords should be changed at least termly.

Passwords should not be re-used and should be made up of a minimum of 8 alphanumeric characters.

They should not be obvious or guessable.

Do not divulge your password to any person, or use another person's password.

Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle or drawer to which only you have access.

Access should only be made to school systems via the authorised account / password, which should not be made available to any other person.

Passwords should be changed immediately if the use believes or suspects that their account has been compromised.

When accessing on-line cloud services such as Office 365 (Files and email) staff should be using school equipment that is only accessible to them. School devices are only for the member of staff that has been allocated the equipment.

If using personal computers, PED's or mobile phones staff are required to ensure that these are password protected and that they fully logout of any work related systems. If this cannot be guaranteed then personal devices should not be linked to work accounts.

Best practice would suggest that software is not used to link multiple accounts e.g. personal and work emails picked up together in Outlook or alternative providers.

Staff & students must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'). Personal data such as SIMs should never be shown through a data projector.

All users should be aware that the ICT system is filtered and monitored.

Data Storage

Staff are instructed to only use encrypted USB drives or hard drives in school. Best practice would suggest uploading files into the schools cloud storage (One drive). If staff are backing up work it should be on an encrypted hard drive using Bit-locker software. Staff are advised not to save work directly to the computer in case the event of theft or due to loss of data.

Reporting

All breaches of the e-safety policy need to be recorded in SIMS as part of the schools behaviour management sanctions. These incidents will be collated by the e-Safety Co-ordinator.

Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately – it is their responsibility to decide on appropriate action not the class teacher's.

Incidents which are not child protection issues but may require SLT/HOY intervention (eg. cyberbullying) should be reported to the SLT lead asap.

Allegations involving staff should be reported to the Headteacher as per the whistleblowing policy. If the allegation is one of abuse, then it should be handled according to the DfE and safe guarding guidelines. If necessary the Local Authority Designated Officer (LADO) should be informed.

Evidence of incidents must be preserved and retained.

The curriculum and assembly programme will cover how pupils should report incidents (eg Child Exploitation and Online Protection (CEOP) button, trusted adult, Childline). The school's website should also be regularly reviewed to provide information to parents regarding e-safety.

Information can be found at:

http://www.oldburywells.com/parent-information/learning-zone-online-safety

Infringements and Sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. Any student in breach of the policy faces the full range of school sanctions including exclusion. A potential guide can be found in **Appendix 5.**

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and collect evidence, the Local Authority Human Resources team and Telford & Wrekin IT Services.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – e.g. class commendation for good research skills, certificates for being good cyber citizens etc. These opportunities are embedded within the curriculum.

The member of the SLT should endeavour to reward any student for outstanding and/or responsible use of ICT in line with the school's rewards policy.

Social networking

Pupils are not permitted to use social networking sites within school.

Staff are only allowed to use social media if it is directly related to their responsibilities/duties.

Best practice would suggest that staff who use social networking outside of school should never comment on school related business and ensure that privacy settings are set to secure or private. These setting should be frequently reviewed.

For teachers, using social media has many benefits in terms of professional networking to improve and support teaching and learning. However, teachers must be aware of the risks. As per the NASUWT recommended guidance the school policy is:

- Do not post anything that could be construed as defamatory or discriminatory against others or the school. Any post can be potentially quoted by the media.
- Do not make or accept friend requests by pupils (current or past) or parents.
- Ensure your privacy settings are adequate. You can determine who sees your posts and most importantly, ensure that you get to approve any pictures in which you may be tagged before the picture is published. You can also disable your profile from certain search engines.
- Any personal social media accounts should not be linked or registered using your work email address.
- When joining or being added to any groups, always check whether it is Public, Closed (where anyone can see the members of the group but not the discussion) or Secret (where neither the members or the discussion are visible).
- Sharing, forwarding or 're-tweeting' can be viewed as a sign of endorsement. This may be inappropriate in some circumstances.
- These guidelines are designed to protect all users of ICT. However, if these rules prevent you from doing your job then permission should be sought from the head teacher in writing. This also includes permission to set up any social media accounts related to school.

Use of Social Media within the School Community

Rationale

Maintaining an online presence is vital for schools, not only in terms of keeping the school community up to date with school events, but also in terms of attracting potential enrolment. Having a school website is an essential part of this, but web users must specifically visit the school website regularly to receive this information. By having a Facebook/ Instagram/

Twitter page, the school is feeding school information, news and notices directly into the personal news feeds of parents and the wider school community.

Aims

The purpose of having a school Facebook/ Instagram/ Twitter Page which is also embedding into the school website is:

- to advance our school information system with shared information, along with the existing methods of letters, text messages, email and the school website.
- to make school announcements and to publicise school events.
- to announce any updated information that appears on our school website.
- to highlight positive school achievements in a forum where they can be shared by the school community.
- as a means of marketing the school to a wider audience.
- to engage the community that OWS serves and to act as a key component of our school's online presence.
- to facilitate communication and networking opportunities between parents especially new or prospective parents.
- to maintain contact with past parents and past pupils.
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

The use of social media is predominately used to communicate. – celebrate successes and sharing school news.

Staff should always assess what the most appropriate method of communication is. For example, social media should never be used for pastoral or individual school issues.

Terms of use of OWS' Facebook/Instagram/Twitter page

The school's social media profile is controlled, moderated and regularly monitored.

- Users should not share anything that may compromise the safety of any member of the school community-never transmit any personal information of pupils, parents or staff.
- Users should not post anything on the page that could be deemed offensive- inappropriate or harmful comments/content will be removed immediately.
- Users should not share any information that is confidential - if it seems confidential, it probably is. Online "conversations" are never private.
- Users cannot tag photographs of children on the page.
- Users should not engage in giving negative feedback on Facebook, it is more appropriate to deal with the school directly on such matters.
- Users will not mention individual staff members in a negative light on the school Facebook page. The tone of any discussions should be positive and respectful.
- Users should not ask to be "friends" with staff as failure to respond may cause offence.
- Users cannot advertise products and services on our school Facebook page. The sanction for breaking any of the terms of use is an automatic ban.

Staff are permitted to follow any of the school's social media feeds but in doing so must ensure that they are operating safely and within the school guidelines.

Staff are permitted to comment on relevant social media feeds, but again in doing so they must ensure that they are operating safely and within the school guidelines.

This links to the social media and communications policy **(Appendix 6)**.

Physical Security of Equipment

Ensure that equipment is sited so as to avoid environmental risks, eg dust, heat. This also applies to official equipment used at home. Ensure that items are kept securely following reasonable precautions to prevent loss, damage or theft.

Staff are issued with computer resources based upon their role. All allocated resource should be kept in good working order. Staff must ensure that equipment is looked after. Any accidental damage must be reported to the network manager immediately and where possible to your house insurance.

If taking resources off site they should only transported in the boot of a car (but not left in boot when parked) and safely secured at home.

Any ICT resources are allocated for business use and must not be used by non-TrustEd employees.

Staff will be requested to sign for all equipment as part of staff induction.

Room Booking

Pupils and Staff are encouraged to gain as much practical experience of ICT equipment as possible. Staff can access the booking system via the schools IT system.

Block bookings should be avoided to allow other teachers the opportunity to book at different times of the day.

All equipment must be checked at the beginning and end of each lesson. Any issues must be reported to the schools network manager.

Under no circumstances should students be left unattended in any computer room.

Software

Staff must not add software onto the school system without consulting the ICT Network Manager.

Any software that requires personal data of students or staff should not be purchased prior to checking with the Data Protection Officer to ensure GDPR regulations are followed. If guarantees cannot be made, then the software will not be used on the schools IT system.

Staff must ensure that all software is updated as per the requests of the network manager to ensure security of the system.

Emails

Personal email use may occasionally be used, however this use should be infrequent and marked 'personal'. No school related business should be communicated through personal email.

All communications should be via the school email system.

The content of all email accessed in school or generated by the school's email system may be checked under the direction of the Head Teacher.

All members of the school community are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) 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.

To balance the quantity of emails and workload the school communication policy outlines the timeline for responding to emails **(APPENDIX 6)**

This guidance aims to enhance the use of email as part of the portfolio of communication media and develop good practice in the use of email as an effective medium of communication.

Sending Emails

Before sending emails consider:

- The maintenance of the highest professional standards – think about how they could be read.
- Whether email is the correct medium for communication.
- To whom should the email be sent, consider expected communication style.
- Only copy in people who have an immediate need for the information. Whole school or All Staff emails should be avoided where possible.
- Please consider the sensitivity of the email topic. Best practice would be to upload the information to shared areas on the L drive or to password protect confidential information prior to attachment.
- The length of the email, avoid long detailed emails.
- Always check the recipients of your email – Best practice is to write the email first and then add the email address in. Staff should also take care in using the Reply all function.
- The use of a digital signature to identify OWS employees.

In the case that emails are sent to the wrong address that contain personal information Staff must attempt to recall the email using the recall tool. If this is unsuccessful as

part of GDPR the Schools data protection officer must be informed. This is a legal requirement.

Always read and check your email before sending.

Receiving and Managing Emails

- Staff should become 'responsible communicators' i.e. they should check their emails at the start of each day as they currently would their pigeon trays.
- Consider whether they need you to respond, retain print and/or delete.
- If they require retention, place emails and attachments in folders. Emails should not be used as a storage area for information. School emails will automatically be deleted from the system in line with the school's data retention policy.
- If they require response, consider carefully the use of the "reply to all" button.
- Delete unwanted emails promptly.
- Protect yourself from viruses when emailing from home or from email addresses that are unrecognised and that contain attachments.

Sensitive Information

- Emails are the electronic equivalent of a postcard. Anyone can read the content along the delivery path. Sensitive information should be sent by post or via a secure transfer system.
- Child Protection issues should not be reported via email.
- Never email in haste, consider the facts and consequences of the message.
- Be professional and careful about what you say about others, as email is easily forwarded. Only put in writing what you would say to someone's face.
- Be aware of copyright and libel issues e.g. when sending scanned text, pictures or information downloaded from the internet.
- An email can be contractually binding therefore care should be taken when expressing personal views that these cannot be misinterpreted as belonging to Trust or LA, as the email address will part contain the Trust or LA name.
- If an urgent email is sent, you may want to follow this with a phone call.
- Never send emails that are offensive, threatening, defamatory or illegal. Emails have been used successfully as evidence in libel cases.
- Emails can be requested as part of the GDPR process, as they can be contractually binding they should be factual. If it is an opinion, then it should be phrased as this in the email.

Security

- Staff are responsible for the security of their computer, and for protecting any information or data used and/or stored on it.
- Do not to leave a mailbox open and unattended, always keep it password protected. The account holder/s needs to strive to keep their passwords confidential; to prevent other users from accessing and sending emails from their account. Users may need to make their passwords known in the event of absence.
- Staff should be responsible for changing passwords on an agreed schedule to maintain security.
- Emails will only be monitored by the Head teacher in very exceptional circumstances.

- Longer term absent staff are aware that their email account may be opened by another member of senior staff. This will only be done with the head teachers authorisation.

The role of email is also covered in the schools communication statement (Appendix 6).

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in online safety/digital literacy is therefore an essential part of the school's/academy'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.

Pupils

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

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should 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.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils should 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. N.B. additional duties for schools/academies 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.
- Students/pupils should be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that students/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.
- Where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. (The internet is always filtered)
- It is accepted that from time to time, for good educational reasons, students 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 period of study. Any request to do so, should be auditable, with clear reasons for the need.

Staff

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.*
- *The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions, with importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in several ways:

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

Monitoring and Reporting

a) The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers.

b) The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

c) The school action plan indicates any planned action based on the above.

Technical – Infrastructure/Equipment, Filtering and Monitoring

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

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the schools IT network manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher/Principal or other nominated senior leader and kept in a secure place (e.g. school safe).
- The ICT Network manager 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. 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 change.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, 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 devices are protected by up-to-date virus software.

Distance Learning

At times the school may need to operate remote learning to continue to deliver the school's curriculum. In this case all communication must be through approved school systems:

- Show My Homework (Satchel One)
- Microsoft Teams
- GCSEPod

All use of these systems is monitored and is only accessible through school issued accounts.

To allow for the delivery of live lessons/content the school has set out expectations in relation to Microsoft Teams.

Parents

- When Microsoft Teams events are scheduled – they will be calendared (appear with at least 24 hours notice) and also content will be identified in Show My Homework.
- If your child is taking part in a Teams lesson, they will receive an email from the teacher (at least 24 hours in advance) which will include the date and time date of the lesson.
- Microsoft Team lessons will be recorded and used subsequently with students who missed the initial session. (This content will not be shared outside of the school community and will ensure safety for all users).
- Please identify a suitable location for your child to use for the video lesson for example a living room or dining area. Bedrooms should not be used.

    1. Parents should ensure that as far as possible distractions are removed and there is quiet.
    2. Parents should make every effort to support lessons delivered in this way by ensuring their child is suitable dressed, prepared and ready to learn.
    3. Parents should familiarise themselves with the expectations on pupils set down in this guidance and ensure their child adheres to them.
    4. Parents are responsible for ensuring that the privacy of other family members is maintained during video sessions.
    5. Remember, lessons delivered online are still lessons and pupils are expected to present themselves and behave appropriately. High standards of behaviour are expected for online learning sessions just as they are in the classroom.

Teachers

- Teachers will ensure that they provide students with at least 24 hours' notice before engaging in Microsoft Teams meetings. All meetings are calendared.
- Teachers will only use school approved video conferencing platform Microsoft Teams.
- Teachers will only use Microsoft Teams using their provided school email address (@oldburywells.com)
- Teachers will record their sessions to ensure safety for all users and for those who may have missed the session.
- Teachers will keep a record of each Meet online (Date, time, length, attendees, topics).
- Online Meets will be kept to a reasonable time period, as devices and Internet may be in high demand at home. (Sessions should be no longer than the timetabled lesson).
- Teachers will ensure students join the Meet with camera and microphones muted on entry.
- Teachers will ensure students abide by the School's Internet Acceptable Usage Policy at all times and pass on any infringements.
- Teachers must conduct sessions in a professional manner, including being suitably attired during online sessions and ensuring they are broadcast from an appropriate location.
- If broadcasting content from home the background should be blurred or altered via the screen settings.

- It is not compulsory for teachers to share their face. If staff feel uncomfortable then alternatives such as sharing resources and talking over that with the chat function on is appropriate for live learning.
- Where possible, video cameras should be used against a neutral background, with the light source directed towards the instructor's face.
- It is recommended teachers wear audio headsets, if possible (to limit audio interruptions during conferencing sessions).
- At the end of a session the teacher must advise all students to leave the session and when all students have left the Meet, the teacher can then end the video conferencing session and terminate the meeting.

Students

- Will only use school technology systems for the purpose of education.
- Treat your video conference as you would a lesson. Be on time and be prepared.
- Be ready to learn and make sure you have class resources, pen/paper etc. at hand.
- Make sure you are in a suitable location; your device is charged (or plugged in) and that you are suitably dressed prior to the beginning of each scheduled video conference.
- Ensure your video is switched off and your microphone is muted until a member of staff instructs you otherwise,
- If possible, you should wear a headset (ideally with a microphone) but this is not essential.
- Remember to behave as you would in school and abide by the school's normal rules.
- Chat functions should be used to ask questions and to answer teacher questions. Please use chat functions responsibly and sensibly. Remember anything you write is recorded.
- Do not record or take photos of your teachers or classmates during live sessions or share sessions via social media.
- Listen, focus on the lesson and learn.
- Avoid distractions such as your mobile phone etc.
- Respect your teacher, your fellow learners and yourself by doing your best just as you would in class.
- Remember your school are putting these lessons on for your benefit but not everyone who tries to contact you online has your interests at heart. If you have any worries or concerns about something that has happened to you on-line, please let the school know immediately.

These rules are set to keep all users safe and everyone has a responsibility to ensure that the are followed. If you misuse or disrupt the learning through Microsoft Teams you may lose your entitlement to participate in these sessions.

Appendix 1

Acceptable Use Policies (AUPs)

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. These technologies can stimulate discussion, promote creativity and stimulate 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 and volunteers 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;
- that young people will be responsible users and stay safe while using the internet and other digital 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 will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

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

Student/Pupil Acceptable Use Agreement

Acceptable Use 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.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line or any part of the school IT system.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school* systems or devices for non-educational purposes.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones/USB devices etc) in school if I have permission and I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites within school.

When using the internet for research or recreation, I recognise that:

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

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

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information whilst using the school ICT systems).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school);
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.;
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email;
- Office 365, Microsoft Teams website etc.

Name of Student/Pupil: .... Group/Class: ....

Signed: .... Date: ....

Staff (and Volunteer) Acceptable Use Policy Agreement

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 students/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, VLE 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.
- 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 relevant member of SLG.

I will be professional in my communications and actions when using *school/*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. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured. I will always check permissions as per the school records (SIMS)
- I will not use social networking sites in school. Only those staff with responsibility for marketing and as authorised by the Headteacher can use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems (@oldburywells.com). Any such communication will be professional in tone and manner.
- I will not share my personal home accounts/data (social media, email etc) with pupils.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- I will avoid using my mobile devices in front of students. When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems (@oldburywells.com only).
- 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 that my data is regularly 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, terrorist or extremist 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 (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users 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 policies.
- 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 School/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in safe storage.
- I understand that data protection policy requires that any staff or student/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 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 that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download 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 agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/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 (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ....

Signed: .... Date: ....

Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

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

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices.

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 (in school and when carrying out communications related to the school) within these guidelines.

Name: ....

Signed: .... Date: ....

Appendix 2
School Registration Form (photos & ICT access consent)

	PUPIL REGISTRATION FORM – Sept 2023
	CONFIDENTIAL PERSONAL DETAILS FOR YOUR CHILD

Childs' Name: …………………………………………

Please find all information pertaining to this Pupil Registration Form, IT consent form and Biometric consent form in the attached booklet, which should be retained for your information.

Birth Certificate:

Please could you provide school with a <u>copy</u> of your child's birth certificate (or a copy of your adoption certificate details where the original birth certificate is no longer relevant). This is simply to ensure that the correct legal name and date of birth is on the school's database. If you wish, we can take a copy of your original certificate, just ask at reception. This is a request not a legal obligation. If you want your child to be "known as" another name, please fill in tab 3 and/or 4. However, please note that the "known as" name cannot be used on certain aspects of our school system or on legal documents such as exam certificates.

Adopted from Care:

You may be aware that children adopted from care on or after **30 December 2005**, as well as those who left care under a special guardianship order or residence order (now known as a child arrangements order) attract a significant sum of additional funding to schools to be used to help support your child's academic progress and attainment.

If this is applicable to your child, we would be grateful if you could indicate (*with a tick*) which category below he/she falls into. It should be emphasised that the offering of this information is purely voluntary, and parents are under no obligation to do so. If ticked we would ask for supporting paperwork, by way of a photocopy of the adoption order. Please feel free to block out any sensitive information e.g. birth parents if you do not wish this to be revealed to the school.

Many thanks for your assistance with this information. Should this apply to you we would be grateful if you could tick below and return any supporting paperwork along with this registration form.
………..
I confirm that my child is adopted, and I have ticked the relevant box **and** provided a copy of the adoption order.

☐	Ceased to be looked after through adoption
☐	Ceased to be looked after through a Special Guardianship Order (SGO)
☐	Ceased to be looked after through a Residence Order (RO)
☐	Ceased to be looked after through a Child Arrangement Order (CAO)
	Supporting Paperwork is provided **Yes** ☐ **No** ☐

For Office Use Only:

Date Received:		
Date entered on SIMS		
Birth Certificate		
LAC		
FSM		
Admission No:		

Please print all details clearly

1.	Your child's Legal Surname	
2.	Your child's Legal Forename(s)	
3.	Your child's "known as" Surname *only complete if this is different from 1 above.*	
4.	Your child's preferred forename	
5.	Your child's date of birth (DDMMYYYY)	
6.	Your child's gender	Male ☐ Female ☐
7.	Your child's full address	…………………………………………………………………………………… …………………………………………………………………………………… …………………………………………………………………………………… ……………………………………………………………………………………
8.	Postcode (**please print**) NB: this must match that on the Post Office website, as the correct postcode is important. Insert a space where necessary (e.g. SY22 5JH).	

Please note that text messages will be sent to Priority 1 contact.

	CHILD'S PARENT/CARER DETAILS - Priority 1 This should be the Parent/Carer with whom your child resides for the majority of the week. If parents are separated but both have contact please provide full details. **Priority 1 contact will be used for message alerts.**	
9.	Relationship to child	
10.	Title & Surname	
11.	First name	
12.	Full address (*only if different from No. 7*)	………………………………………………………………………… ………………………………………………………………………… ………………………………………………………………………… …………………………………………………………………………
13.	Postcode (*see note in 8 above*)	
14.	Mobile telephone number This number will be used for text messaging.	
15.	Work telephone number	
16.	Home phone number	
17.	Email address (we will not divulge to any third party). Please print this in capital letters.	Home:………………………………………………………………… Work: …………………………………………………………………

	CHILD'S PARENT/CARER DETAILS – Priority 2	
18.	Relationship to child	
19.	Title & Surname	
20.	First name	
21.	Full address (*only if different from No. 7*)	……………………………………………………… ……………………………………………………… ……………………………………………………… ………………………………………………………
22.	Postcode *(see note in 8 above)*	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
23.	Mobile telephone number	
24.	Work telephone number	
25.	Home phone number	
26.	Email address (we will not divulge to any third party). Please print this in capital letters.	Home:……………………………………………………… Work: ………………………………………………………
27.	Are either Parent/Carer a member of the armed forces? Please tick Yes or No. (Your classification will be either PStat Cat 1 or 2; please note this only refers to regular forces and not the territorial's.)	Parent/Carer 1: Yes ☐ No ☐ Parent/Carer 2: Yes ☐ No ☐
	In case we cannot reach either Parent/Guardian please provide an emergency contact who can act for you.	
	Priority 3 - Emergency Contact	
28.	Relationship to child	
29.	First name	
30.	Title & Surname	
31.	Full address	……………………………………………………… ……………………………………………………… ……………………………………………………… ………………………………………………………
32.	Postcode *(see note in 8 above)*	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
33.	Home telephone number	
34.	Work telephone number	
35.	Mobile phone number	

	Priority 4 - Emergency Contact	
36.	Relationship to child	
37.	First name	
38.	Title & Surname	
39.	Full address	…………………………………………………………………… …………………………………………………………………… ……………………………………………………………………
40.	Postcode *(see note in 8 above)*	
41.	Home telephone number	
42.	Work telephone number	
43.	Mobile phone number	
44.	Is your child currently in receipt of Free School Meals *(please tick)*	**Yes** ☐ **No** ☐ *If you are out of area and receive FSM you will need to make an application to Shropshire County – please ask for an application form.*
45.	Does your child have any **medical condition** (including asthma* or allergies) that we need to be aware of? If so, please provide full details including any medication that is being taken orally or by injection.	…………………………………………………………………… …………………………………………………………………… …………………………………………………………………… …………………………………………………………………… …………………………………………………………………… …………………………………………………………………… ** If your child has asthma please tick under the <u>Parental Consents</u> for use of an emergency inhaler if personal inhaler has been forgotten.*
46.	Please give the name of your child's **Medical Practice** <u>***NOT***</u> *your doctor's name.*	**Name of Medical Practice**: …………………………………………………………………… Phone No: ………………………………………………………
47.	**Consent for Emergency Medical Assistance** (If you circle 'No', please let the school have details as to what you would not allow under this consent).	Yes ☐ No ☐

Ethnic/Cultural

On the next couple of pages, we ask you about your child's Ethnicity, Religion, Mother Tongue and language and how your child normally travels to school. We know that some parents/guardians are concerned about identity theft but rest assured that whenever we do transfer any information to other parties it is done through totally secure networks. You have every right to refuse to give any of the following information. However, if you complete each section, it may result in additional resources for the authority and the school. In relation to the mode of travel please be honest about this and where, for example, part of the journey is by car and part, say, is walking, please list the mode of transport used for the majority of the journey to school. This information can be used to great advantage for us when working on School Travel Plan and with Shirehall colleagues in obtaining funding for Safer Routes to School.

(A) Ethnicity (based on the Census ethnic categories)

Our ethnic background describes how we think of ourselves. This may be based on many things, including, for example, our skin colour, language, culture, ancestry or family history. ***Ethnic background is not the same as nationality or country of birth.*** Please study the list below and tick <u>one box only</u> to indicate the ethnic background of your child.

White
- ♦ English ☐
- ♦ Scottish ☐
- ♦ Welsh ☐
- ♦ Cornish ☐
- ♦ White Eastern European* ☐
- ♦ White Western European** ☐
- ♦ Other White British ☐
- ♦ Irish ☐
- ♦ Traveller of Irish Heritage ☐
- ♦ Gypsy/Roma ☐
- ♦ Any other White background ☐

Mixed
- ♦ White and Black Caribbean ☐
- ♦ White and Black African ☐
- ♦ White and Asian ☐
- ♦ Any other mixed background ☐

Asian or Asian British
- ♦ Indian ☐
- ♦ Pakistani ☐
- ♦ Bangladeshi ☐
- ♦ Any other Asian background ☐

Black or Black British
- ♦ Caribbean ☐
- ♦ African ☐
- ♦ Any other Black background ☐

Chinese ☐

Any other ethnic background ☐

I DO NOT wish to give this information ☐

* White Eastern European includes those from Belarus, Bosnia & Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Macedonia, Moldova, Poland, Romania, Russia, Serbia & Montenegro, Slovak, Slovenia and Ukraine. ** White Western European includes those from Austria, Belgium, Denmark, Finland, France, Germany, Holland, Italy, Luxembourg, Malta, Norway, Portugal, Spain, Sweden and Switzerland.

(B) <u>First Language</u>

"Mother tongue" or first language is the language to which your child was initially exposed during early development and continues to use this language in the home or the community. If a child acquired English, subsequent to early development, English cannot be denoted as their mother tongue no matter how proficient they have become. On this basis, please would you tick the appropriate box for what you therefore consider to be your child's mother tongue:

1. English ☐

2. Other than English ☐

(2a) *If you ticked 2 above, please would you tell us the most appropriate language you regard as your child's first language? (If we are unable to find this on our extensive listing of languages we may contact you for further clarification).*

....

3. I DO NOT wish to give this information ☐

(C) Home Language

Please state your child's home language, which is mostly used in the home or in the community:

...

(G) <u>Please would you let us have your family's religion by ticking one box below?</u>

Christian ☐	Anglican ☐	Baptist ☐	Methodist ☐
Catholic ☐	Hindu ☐	Jewish ☐	Muslim ☐
Sikh ☐	Buddhist ☐	No Religion ☐	Other Religion ☐

I DO NOT wish to give this information ☐

<u>Mode of travel to school</u>

Please tick the <u>predominant mode of travel</u> for your child – please tick ONE box only:

1. Bus – type not known *(see 5 or 6 as alternatives)*	☐ **BNK**	6. Public Service Bus *	☐ **PSB**
2. Car or Van	☐ **CAR**	7. Taxi	☐ **TXI**
3. Car Share *(with child/children from a different dwelling)*	☐ **CRS**	8. Train	☐ **TRN**
4. Cycle	☐ **CYC**	9. Walk	☐ **WLK**
5. Dedicated School Bus *	☐ **DSB**	10. Other	☐ **OTH**
		Please specify……………..………………..	

* Note – a public service vehicle will always have a service number, a dedicated school bus will not. If you are involved in a park and stride service this needs to be ticked as <u>Car</u> and not Walk. Mode of travel information is vital for School Travel Plans and it is the parents/guardian's responsibility to notify the school immediately if mode of travel changes.

Previous School	
Name:	………………………………………………………………
Address:	………………………………………………………………
	………………………………………………………………
	………………………………………………………………
Phone Number:	………………………………………………………………
Start Date:	………………………………………………………………
Leaving Date:	………………………………………………………………
Headteacher:	………………………………………………………………
Class Teacher:	

PARENTAL CONSENTS
WE NEED YOUR PERMISSION FOR CERTAIN ASPECTS OF YOUR CHILD'S EDUCATION

Please would you tick **Yes** or **No** as appropriate, thank you.

	Yes	No
Permission to receive Paracetamol whilst at school	Yes ☐	No ☐
Permission to use an emergency inhaler ***Only*** *if your child has been diagnosed with Asthma*	Yes ☐	No ☐
Accessing the internet at school	Yes ☐	No ☐
Photograph in our school prospectus/marketing	Yes ☐	No ☐
Photograph on our school website/social media	Yes ☐	No ☐
Photograph in our school newsletter	Yes ☐	No ☐
Photograph in the local press (to include sporting events)	Yes ☐	No ☐
Video Imaging (i.e. school productions)	Yes ☐	No ☐
School Photographs	Yes ☐	No ☐
Copyright permission of any work produced e.g. for displays, competitions, articles etc.	Yes ☐	No ☐
Sex Education as part of Personal, Social, Health and Economic education	Yes ☐	No ☐

Home-School Agreement

From the start of my time at Oldbury Wells School, I will commit myself to doing my best to carry out the agreement as set out below.

Signed by:

Student .... Form ....

Parent/Carer .... Date ....

....

The School will support Parents and Students by:

- Maintaining a good quality of education, with high expectations for all the School's students and offering sound advice and encouragement about careers and higher education.

- Monitoring and keeping parents informed on children's progress and any problems which may arise.

- Providing assistance from the School's Special Educational Needs Co-ordinator where any child may need additional support.

- Responding promptly to parental worries, concerns or complaints with respect and sensitivity.

- Encourage children to attend school regularly and punctually and by contacting you if we are concerned about any aspect of this.

- Maintaining strong policies on bullying, smoking and general discipline, in particular supporting children who have problems with others.

- Providing a positive, happy and safe working atmosphere.

- Providing an education that covers spiritual, moral, cultural and social development, including sport and extra-curricular activities, as well as academic matters.

- Consulting parents over important changes to school policies.

- Maintaining strong policies on ICT use and misuse.

- Work with professionals from other agencies to promote student welfare education.

Parents will support the School and Students by:

- Avoiding taking holidays in term-time, except in exceptional circumstances.

- Ensuring the highest possible levels of timekeeping and attendance and notifying the School promptly of absence.

- Supporting the School's policy on uniform.

- Understanding the School's need for good behaviour and helping the School by explaining its decisions to their children.

- Providing appropriate study facilities for home learning and ensuring that children tackle tasks thoroughly.

- Taking an interest in their children's work (the School welcomes parental help for children).

- Attending parent's evenings to discuss their children's progress.

- Contact school if a child is worried about attending school or if something happens to affect a child's learning.

- Ensure that school books are kept in good condition and that textbooks are handed back in good condition at the end of the academic year.

- Supporting the standards set by the School for their children to follow when using media and information sources, such as the Internet.
- Supporting the school in promoting responsible, good behaviour to and from school.

Students will support themselves and other students by:

- Doing their best for themselves in the classroom by trying their hardest at all times, tackling difficulties and asking for help.
- Respecting others in the classroom by getting on with their own work quietly and helpfully.
- Being kind, honest and thoughtful in their treatment of all others.
- Respecting the school environment - its grounds and buildings - and keeping it tidy.
- Always doing "politely, at once and without fuss" as asked by any member of staff.
- Taking pride in being members of Oldbury Wells School and upholding its good name by their appearance and behaviour.
- Recognising and valuing the ways in which their parents can help them.
- Promoting the safety and wellbeing of other members of the school community through responsible and careful behaviour.
- Abiding by policies, which also promote safety and well-being, such as ICT use and misuse, behaviour policy, home learning policy etc.

Governors

As Governors of the school, we will do our best to:

- Seek financial efficiency and value for money
- Draw up and publish a full set of school policies and ensure they are up to date
- Consult with and report to parents/carers
- Ensure compliance with statutory obligations, including health and safety regulations
- Monitor and review all aspects of the school's work.

Alan Edwards
Chair of Governors

The School will continue to monitor, review and evaluate this agreement for its effectiveness and improvement, and will ensure that parents and students are involved in this process.

Lee Tristham
Headteacher
Sept. 2023

IT Consent Form

I have read and understand the Oldbury Wells ICT, Data Security Policy, which is contained within the Information and Guidance notes, and I agree to abide by the terms and requirements of those policies.

Both Parent/Guardian and Pupil should sign below:-

Signed: (Parent)……………………...........…………….(Pupil)………………………………………

Print Name: (Parent) ……………………………………….. (Pupil)…………………………………………..

Date: …………………………

Also:

Where pupils are under the age of 13, we require a Parent/Guardian to give consent that they are allowed to use websites linked to teaching and learning e.g., careers guidance software. These are checked by teachers and do not require full pupil data, but they may require a pupil's name.

Consent given: Yes ☐   No ☐

Biometric Consent Form

I confirm that I wish my child /children   **TO BE** ☐   **NOT TO BE** ☐   (*please tick*)

registered on the school's Biometric Cashless Catering System with immediate effect.

I understand that **I** may withdraw my child's registration at any time in writing. If you choose 'not to be' your child will be issued with a PIN number.

Child/Children's Name	Relationship to Child/Children

Youth Support Services

Once a student has turned 13, schools have to provide details to the Youth Support Services. The Youth Support Service is the Local Authority's advice and information service for all young people aged between 13 and 19, e.g. careers advice. Schools have to provide student names, DOB and addresses, names and addresses of both parent(s). However, schools may also be asked to provide further information about students to the Youth Support Services that is relevant to their work. Under the General Data Protection Regulation (GDPR) parents have the right to choose whether or not they would be happy for school to release the further information about their child beyond the statutory information outlined above.

Consent given: Yes ☐   No ☐

Signed: (Parent)……………………………...........……………..

Print Name: (Parent) ……………………………………….. 				Date: …………………………

> Please note it is the parents/guardian's responsibility to notify the school immediately if any of the information on this registration form changes

PLEASE SIGN BELOW AND RETURN COMPLETED FORM TO:

Miss E Woodward
Admissions Administrator
Oldbury Wells
Bridgnorth
WV16 5JD

FORMS TO BE RETURNED ASAP PLEASE

I acknowledge that the details and information I have provided must only be used for the purposes indicated by pages 3-6 of the Information and Guidance Booklet.

Signed: …………………………….…............…. Parent/Guardian   Date: …………………………

This document can be made available in other formats, e.g. Braille, as well as other languages. Please tell us if that is the case and we will make arrangements with Shirehall to ensure that you receive one as soon as possible. Please note that documents requested in other languages can take between four and six weeks to supply.

APPENDIX 3

Staff Summary sheet IT Update linked to GDPR

Oldbury Wells School – ICT & GDPR Summary Guide for staff

The full ICT & E-Safety policy can be found on the school's website.

Do

- Always inform the E-Safety co-ordinator (SW) of any issues. These will be recorded and reviewed to ensure further improvements.
- Always review and update your password termly. These should be strong (8 characters and contain numbers and letters)
- Ensure that your allocated school device (laptop/i-pad) is only used by yourself and only for school related business.
- If your mobile phone or personal computer is linked to your Office 365 account you must ensure that you are the only person who has access to this. Check that you have logged out correctly and that you have not downloaded any sensitive data to your device. The device must be password protected.
- Check the register of consent in SIMS if you want to take/use a photo of a student.
- Please ask any visitors to school to ensure that mobile phones are switched off.
- Only use encrypted USB or encrypted hard drives to store personal data – best practice is to use the cloud (Office 365).
- If transporting ICT equipment off site this must be transported in your boot and not left in it overnight. It is your responsibility to ensure they are stored safely and securely at home.
- The school recommends that the use of social media accounts is limited to protect yourselves.
- If you have social media accounts check them to ensure privacy settings are robust.
- Protect yourself if you use social media by not accepting friend requests from parents, pupils (current or former). If you need to do this then please write to the Headteacher outlining your reasons.
- Remember that sharing, forwarding posts or emails can be viewed as a sign of endorsement.
- Check any groups that you may join – if it is open does it contain pupils, parents?
- When sending email:
  - Check the correct recipients
  - Write it in a professional manner
  - Always write the email first and then add the address
  - Take care if you 'reply all'
  - Use digital signature strip
  - If you accidently send the email to the wrong address try to retrieve it. If this is not possible then you MUST inform the schools Data Protection Officer.
- When receiving emails:
  - Check the address and never open unfamiliar emails in the event of a virus or malware.
  - Check regularly and delete unwanted emails promptly. If files are important they should be saved to the cloud drive and not on the email system to reduce risk of a data breach.
- Remember that an email can be contractually binding, therefore take care if expressing your opinion.

- If you take pupil information home (planning folders, pupil files) you must do this in a secure manner. It should be transported in a separate bag in your boot. When at home these must not be left in the boot but secured safely. Any files that are taken home must have a copy of the schools contact details if found.
- In school pupil information should be stored securely in lockable drawers, locked filing cabinets and offices.

If you feel that there has been a data breach you must inform the schools Data Protection Officer immediately

Don't

- Leave your laptop unlocked in school (Control – Alt – Delete to lock) this has the potential to be a data breach if pupils can access emails or Sims. These should never be broadcast through a projector.
- Divulge your password to anyone else. These must be changed immediately if you feel that your account has been compromised.
- Install software onto your device without contacting the ICT Network Manager.
- Purchase software that requires personal data of students without checking with the Data Protection Officer to ensure GDPR compliance. If it is not compliant it will not be installed.
- Use your own personal devices to take pictures of pupils or to phone text parents – if you need to these must be removed as soon as possible and stored on the school's cloud system.
- Share personal contact details with parents such as personal emails or phone numbers.
- Use social media to discuss school related business at all that may be construed as defamatory or discriminatory.
- Register any social media accounts to your school account @oldburywells.com
- Send sensitive data via email to an unknown contact – Best practice would be to use encrypted email or to password protect a document and then phone the recipient with the password.
- Accept friend requests from parents, pupils or past pupils. Block any requests of this type.
- Give personal information to a third party without checking (even from the police)
- Leave sensitive data in staff pigeon holes – always pass face to face.

Remember these guidelines are set to protect all users from any breaches or misuse of ICT equipment, and systems.

Appendix 4

Mobile & Communication Technologies

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

*1

Appendix 5

Sanctions

Dealing with unsuitable/inappropriate activities

It is rare for any inappropriate activity to occur as the schools blocking system will prevent this, but if it was to occur:

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and /or illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	

	1	2	3	4	5
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce			X		
File sharing			X		
Use of social media (Only designated staff can use school social media feed)				X	
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube (live streaming)				X	

In the more serious incidents outlined above, action may be taken outside of the school and directed by the police or Local authority designated officer (LADO).

These actions above also link to the schools code of conduct.

Other Incidents

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

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

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

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

(This is a guide and at times circumstances may dictate a change in action/sanction)

Students/Pupils Incidents	Actions/Sanctions								
	Refer to class teacher/tutor	Refer to Head of Department/Year/other	Refer to Headteacher/Principal	Refer to Police where appropriate	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X				X	X		X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X				X		X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email		X		X		X	X	X	X
Unauthorised downloading or uploading of files		X			X	X	X	X	X
Allowing others to access school network by sharing username and passwords	X				X	X	X	X	X
Attempting to access or accessing the school network, using another student's/pupil's account			X		X	X	X		X
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X		X
Corrupting or destroying the data of other users			X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X	X	X

	1	2	3	4	5	6	7	8
Continued infringements of the above, following previous warnings or sanctions	X				X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X			X
Using proxy sites or other means to subvert the school's/academy's filtering system	X			X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X				X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X				X		X

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

Appendix 6
Social Media & Communication Statement
Updated July 2020 – social media

1. Introduction and Aims

We believe that clear, open communication between the school and parents/carers has a positive impact on pupils' learning because it:

- Gives parents/carers the information they need to support their child's education.
- Helps the school improve, through feedback and consultation with parents/carers.
- Builds trust between home and school, which helps the school better support each child's educational and pastoral needs.

The aim of this policy is to promote clear and open communication by:

- Explaining how the school communicates with parents/carers.
- Setting clear standards for responding to communication from parents/carers.
- Helping parents/carers reach the member of school staff who is best placed to address their specific query or concern so they can get a response as quickly as possible.
- Setting safe boundaries for the use of social media as a communication tool.

In the following sections, we will use 'parents' to refer to both parents and carers.

2. Roles and Responsibilities

2.1 Headteacher

The headteacher is responsible for:

- Ensuring that communications with parents are effective, timely and appropriate.
- Regularly reviewing this policy.

2.2 Staff

All staff are responsible for:

- Responding to communication from parents in line with this policy and the school's ICT and internet acceptable use policy.
- Working with other members of staff to make sure parents get timely information (if they cannot address a query or send the information themselves).

As a school we do not expect teachers to respond to communications outside of school hours 8.30am - 4.30pm, or their working hours (if they work part-time), or during school holidays.

Please note that senior members or key members of staff will always aim to contact parents as soon as possible if there are any issues related to pupil welfare.

Ordinarily, staff will aim to not contact other members of staff via email outside of the hours 8am till 6pm. Staff are not expected to check emails outside of these hours.

2.3 Parents

Parents are responsible for:

- Ensuring that communication with the school is respectful at all times.
- Making every reasonable effort to address communications to the appropriate member of staff in the first instance.
- Respond to communications from the school (such as requests for meetings) in a timely manner.
- Checking all communications from the school.
- Ensuring that contact details are up to date.

3. How We Communicate with Parents and Carers

The sections below explain how we keep parents up-to-date with their child's education and what is happening in school.

Parents should monitor all of the following regularly to make sure they do not miss important communications or announcements that may affect their child.

3.1 Email

We use email to keep parents informed about the following things:

- Upcoming school events
- Scheduled school closures (for example, for staff training days)
- School surveys or consultations
- Class activities or teacher requests
- Copies of school letters/newsletters

3.2 Text Messages

We will text parents about:

- Payments
- Short-notice changes to the school day
- Emergency school closures (for instance, due to bad weather)
- Pupil praise and or sanctions.

3.3 School Calendar

Our school website includes a full school calendar for the academic year.

Where possible, we try to give parents at least 2 weeks' notice of any events or special occasions (including non-uniform days, special assemblies or visitors, or requests for pupils to bring in special items or materials). Any such event will be included in the school calendar.

3.4 Phone Calls

The school encourages teachers to actively call parents to discuss issues/sanctions or praise. Likewise, parents are encouraged to contact the school by phone, but must be aware that due to teaching commitments it may take teachers longer to return any calls.

The school aims to acknowledge all initial calls within 2 working days.

3.5 Letters

We send the following letters home regularly:

- Letters about trips and visits
- Consent forms
- Our termly newsletter

3.6 Homework /Satchel One

All pupils have access to Satchel One (online platform) which allows all homelearning to be set by staff and monitored effectively. Staff are asked to monitor completion of homework and apply school policy to recognise successful outcomes or to pick up other homelearning concerns.

3.7 Reports

Parents receive reports from the school about their child's learning, including:

- A short data capture that outlines the pupils current working at grade and attitude to learning grades (Effort, Behaviour & homework) and their attendance.
- A fuller data capture that outlines the pupils current working at grade and attitude to learning grades (Effort, Behaviour & homework) and their attendance. This report also contains a written comment from the students teacher and Head of Year.
- We also arrange regular meetings where parents can speak to their child's teacher(s) about their achievement and progress (see the section below).

3.8 Meetings

We hold one parents' evening per year. During these meetings, parents can talk with teachers about their child's achievement and progress, the curriculum or schemes of work, their child's wellbeing, or any other area of concern.

The school may also contact parents to arrange meetings between parents' evenings if there are concerns about a child's achievement, progress, or wellbeing.

Parents of pupils with special educational needs (SEN), or who have other additional needs, may also be asked to attend further meetings to address these additional needs.

3.9 School Website

Key information about the school is posted on our website, including:

- School times and term dates
- Important events and announcements
- Curriculum and extra curricular information
- Important policies and procedures

- Important contact information

Parents should check the website before contacting the school.

3.10 Social Media

Information about the school is posted on the school's social media pages, including:

- Events and announcements
- Celebration of school and pupil successes
- Curriculum and extra curricular information
- Important policies and procedures

4. How Parents and Carers can Communicate with the School

Please use the list in Appendix 1 to identify the most appropriate person to contact about a query or issue, including the school office number and email address.

4.1 Email

Parents should always email the school, or the appropriate member of staff, about non-urgent issues in the first instance.

We aim to acknowledge all emails within 2 working days, and to respond in full (or arrange a meeting or phone call if appropriate) within 5 working days. For formal complaint please see the school's complaints policy found on the website.

If a query or concern is urgent, and you need a response sooner than this, please call the school.

4.2 Phone Calls

If you need to speak to a specific member of staff about a **non-urgent** matter, please email or phone the school office and the relevant member of staff will contact you within 2 working days. We aim to resolve non-urgent matters within 5 working days.

If this is not possible (due to teaching or other commitments), someone will get in touch with you to schedule a phone call at a convenient time. We aim to make sure you have spoken to the appropriate member of staff within 2 days of your request.

We will endeavor to contact you as a matter of urgency if the issue is urgent.

Urgent issues might include things like: Please tell them it's urgent:

- Family emergencies
- Safeguarding or welfare issues

For more general enquiries, please call the school office.

Staff will rarely use their own personal devices to contact parents. In the rare event that this does happen staff will endeavor to ensure that any personal numbers are withheld.

4.3 Meetings

If you would like to schedule a meeting with a member of staff, please email the appropriate address (see appendix 1) or call the school to book an appointment.
We will try and arrange a meeting within 5 working days or sooner, but this can be dependent on teaching commitments.

While teachers are available at the beginning or end of the school day if you need to speak to them urgently, we recommend you book appointments to discuss:

- Any concerns you may have about your child's learning.
- Updates related to pastoral support, your child's home environment, or their wellbeing.

5. Inclusion

It is important to us that everyone in our community can communicate easily with the school.

We currently make whole-school announcements and communications (such as email alerts and newsletters) available in the following languages:

- English
- Parents who need help communicating with the school can request the following support:
    - School announcements and communications translated into additional languages;
    - Interpreters for meetings or phone calls.

We can make additional arrangements if necessary. Please contact the school office to discuss these.

6. Monitoring and Review

The headteacher monitors the implementation of this policy and will review the policy every 2 years. The policy will be approved by the governing board.

7. Social Media

All staff are reminded of their responsibilities under the ICT & E-safety policy.

Use of Social Media

Rationale

Maintaining an online presence is vital for schools, not only in terms of keeping the school community up to date with school events, but also in terms of attracting potential enrolment. Having a school website is an essential part of this, but web users must specifically visit the school website regularly to receive this information. By having a Facebook/ Instagram/ Twitter page, the school is feeding school information, news and notices directly into the personal news feeds of parents and the wider school community.

<u>Aims</u>

The purpose of having a school Facebook/ Instagram/ Twitter Page which is also embedding into the school website is:

- to advance our school information system with shared information, along with the existing methods of letters, text messages, email and the school website;
- to make school announcements and to publicise school events;
- to announce any updated information that appears on our school website;
- to highlight positive school achievements in a forum where they can be shared by the school community;
- as a means of marketing the school to a wider audience;
- to engage the community that OWS serves and to act as a key component of our school's online presence;
- to facilitate communication and networking opportunities between parents especially new or prospective parents;
- to maintain contact with past parents and past pupils.

Terms of Use of OWS' Facebook/Instagram/Twitter Page

- Users should not share anything that may compromise the safety of any member of the school community-never transmit any personal information of pupils, parents or staff.
- Users should not post anything on the page that could be deemed offensive- inappropriate or harmful comments/content will be removed immediately.
- Users should not share any information that is confidential- if it seems confidential, it probably is. Online "conversations" are never private.
- Users cannot tag photographs of children on the page.
- Users should not engage in giving negative feedback on Facebook, it is more appropriate to deal with the school directly on such matters.
- Users will not mention individual staff members in a negative light on the school Facebook page. The tone of any discussions should be positive and respectful.
- Users should not ask to be "friends" with staff as failure to respond may cause offence.
- Users cannot advertise products and services on our school Facebook page. The sanction for breaking any of the terms of use is an automatic ban.

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

The use of social media is predominately used to communicate – celebrate successes and sharing school news.

Staff should always assess what the most appropriate method of communication is. For example, social media should never be used for pastoral or individual school issues.

Points to Note

Facebook lists a minimum age requirement of 13, all parents are reminded that children under the age of 13 should not be on Facebook.

When school staff are wishing to 'follow' school social media platforms with their own accounts, they themselves must adhere to the privacy policy, this includes making sure their profiles are private and their past posts are limited.

To update privacy settings on social media please see:

https://www.digitalspy.com/tech/a552990/how-do-i-make-my-facebook-profile-private/

https://www.wikihow.com/Make-Your-Twitter-Account-Private

https://help.instagram.com/196883487377501

Personal Use

Staff

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Students

- Staff are not permitted to follow or engage with current or prior students of the school on any personal social media network account.
- The school's education programme should enable the students to be safe and responsible users of social media.
- Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school.
- In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Comments Posted by Parents/Carers

- Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.
- School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion.
- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents must not make complaints on social networking sites but through official school channels, to ensure that they can be dealt with appropriately.
- Parents must not post malicious or fictitious comments on social networking sites about any member of the school community.
- In the case of inappropriate use of social networking by parents, the school will contact the parent asking them to remove such comments and seek redress through the appropriate channels.

8. Links with Other Policies

The policy should be read alongside our policies on:

- ICT and internet acceptable use
- Staff code of conduct
- Complaints policy

Appendix 7
School Contact List

Who should I contact?

Option 1:

If you have questions about any of the topics in the table below, or would like to speak to a member of staff:

- Email or call the school office on school@oldburywells.com / 01746 765454.
- Put the subject and the name of the relevant member of staff (from the list below) in the subject line (for emails).
- We will forward your request on to the relevant member of staff.

Remember: Check our website first, much of the information you need is posted there. We try to respond to acknowledge all emails within 2 working days.

Option 2:

If you have questions about any of the topics in the table below, or would like to speak to a member of staff:

- Email the most appropriate address.
- Include your child's full name in the subject line along with their form group.

We try to respond to all emails within 2 working days.

I HAVE A QUESTION ABOUT…	WHO YOU NEED TO TALK TO
My child's learning/class activities/lessons/homework	Your child's [class teacher/ subject teacher/ form tutor] Phone: 01746 765454 or Email: school@oldburywells.com
My child's wellbeing/pastoral support	
Y7/8/9	amy.burrows@oldburywells.com lisa.bridgwater@oldburywells.com
Y10/11:	sarah.barlow@oldburywells.com lucy.goodison@oldburywells.com
Bridgnorth Sixth Form	april.bishell@oldburywells.com tracy.fyfe@oldburywells.com
Payments	finance@oldburywells.com
School trips	school@oldburywells.com
Uniform/lost and found	school@oldburywells.com or Phone: 01746 765454

Attendance and absence requests	If you need to report your child's absence either:
	Phone: 01746 765454 Option 1
	Email: attendance@oldburywells.com
If you want to request approval for term-time absence, contact [school office] or download Leave of Absence Request Form from Website (under Parents)	Download LOA form:
	https://bit.ly/45uG64T
	Phone: 01746 765454
	Email: school@oldburywells.com
School events/the school calendar	School office 01746 765454 or email
	school@oldburywells.com
Special Educational Needs	shirley.anthony@oldburywells.com or
	tom.williams@oldburywells.com

Complaints

If you would like to file a formal complaint, please follow the procedure set out in our complaints policy. This can be found on the school's website.