OLDBURY WELLS SCHOOL

ICT and

General Data Protection Regulation (GDPR)

Supplementary Guidance
during school closure

There are no significant changes to the GDPR regulations or ICT policies. We are reminded that, even in these exceptional circumstances, we still have a role to play in ensuring all personal data is protected and lawful.

All policies in full can be found on the OWS website: http://www.oldburywells.com/information/policies/

An updated risk assessment is attached for the handling of personal data, along with good practice reminders.

GDPR

Risk assessment of personal data of children for Coronavirus

Should the schools close, there will be a need for the Designated Safeguarding Leads (DSLs) to remain in contact with vulnerable children. This may mean personal data going home in electronic or paper files.

There will be a risk as children's personal data, and any information recorded during the duration of closure, will be stored in DSLs' homes, and normally this would not be recommended.

Risks

1) Children's names, address and phone numbers will be stored on paper copies at home
2) All calls made to the families will be recorded on either paper or electronically and may not be able to be taken by to the school during closure.
3) Other family members may be at home due to school closures, business closures or possible infection.

Reasons for data to be stored and recorded

These children are considered to be at risk whilst not at school for many reasons, poverty, neglect etc. We, as schools, have a duty of care during this pandemic to protect and safeguard these children.

The DSLs will be required to contact these families to ensure all is ok, they have food etc.

In light of this we are happy for data to be go home as long as the following is adhered to:

1) Where possible all this is stored and recorded using the cloud.
2) Where paper copies have to go home, that they are signed out from the school by the Designated Lead.
3) The minimum of data is taken home from school and once at home is stored safely at home e.g. in a filing cabinet.
4) Any data recorded about each child is kept to a minimum, eg – Called Parent of SW today they have enough food for a week.
5) Where possible this data is taken to school as soon as is possible and signed back in.
6) That this information is not recorded on any personal devices e.g. Word on a personal laptop.

Data Breach

There are no changes here – If staff believe a data breach has occurred they must contact scott.wycherley@oldburywells.com as soon as possible (at least within 12 hours of the event occurring). The full details of this can be found at http://www.oldburywells.com/media/1425/gdpr-may-18.pdf

However, staff are reminded that whilst working from home sensible precautions can be applied to reduce the risk of a data breach.

- Staff are reminded that any of the school's ICT equipment is for their use only in line with their professional responsibilities/duties.
- Where possible, all records should be recorded electronically.
- If paper copies of files (this should be avoided apart from instructions from the DSL) are used these must be stored securely and contain minimum information.
- All staff should ensure that, when not using ICT facilities, the screen should be locked.
- If any sensitive pupil/staff data is shared between professionals, please check email addresses, where possible password protect a document and share the password via phone.
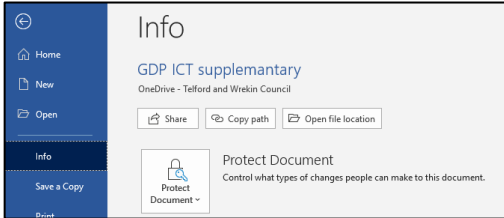
You can also encrypt messages by entering:

Encrypt: *Normal message title here*

Never put the pupils full name in the subject line – please use initials only.

Processing of Personal data

On the 19th March 2020 the European Data Protection Board adopted the following statement:

https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

E-Safety & ICT – Policy can be fund here: http://www.oldburywells.com/media/1424/digital-and-e-safety-policy-2018.pdf

All staff and students are signed up to an authorised user agreement (AUA) – the conditions of these still stand.

All use of school equipment and student accounts are monitored for security, diagnostic and account/audit reasons.

Any loaned equipment has been signed for.

To support distance learning, the rotation of passwords for both staff and students has been suspended. Therefore, staff will not be prompted to change passwords, but if they feel passwords have been compromised, they must contact the ICT team and inform Scott Wycherley immediately.

The school is setting work for students through Show my Homework. This should be the only electronic tool used for the setting of work.

When setting work, staff are to follow the school timetable. (An independent study day has been introduced where staff are not expected to set work – This will be reviewed as we go forward)

The messaging service in SMHW or email should be used to predominately communicate with students. Staff are reminded to adhere to the usual protocols with regards to e-mail communications as per the ICT policy.

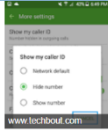Please take care when responding to emails to avoid reply all.

Where staff are required to make phone calls to parents they should ensure that they withhold their numbers:

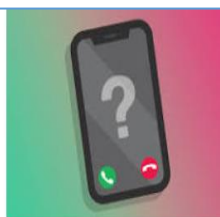Landline: 141 should be entered before entering the phone number

Mobiles: This changes according to phone, but a step by step guide can be found below:

The use of group emails are limited to SLG members. If you need to send an email to all staff, please contact a member of SLG to do this for you.

A member of staff has been given responsibility to support parents/staff with E-safety concerns. brian.lacroix@oldburywells.com

Video Conferencing – There is no expectation that staff film themselves or partake in video conferencing calls with pupils. Teachers are asked not to put themselves in this situation and to protect professional boundaries. In the very rare occasion that this is needed, staff should seek authorisation from Scott Wycherley.

The main secure (video conferencing) tool that the school approves for the communication between staff and groups of staff is Microsoft Teams.

Other communication tools like Zoom are not permitted to discuss school related matters. However, groups of staff can communicate with each other on Zoom or other social media apps, but only for the purpose of touching base and general uncontentious discussion. In these instances, personal accounts/email addresses should be used, and no sensitive or contentious school business discussed, including no discussion about pupils.

All of our main school business and pupil/school related discussions must be undertaken through Microsoft Teams. Pre-arranged groups have been established. If staff wish other groups to be set up, they must contact Andy Thomas and he will help you get started. It's very easy to use and secure.

These are the main issues with Zoom:

1. Each Zoom call has a randomly generated ID number between 9-11 digits long – if someone guessed or used brute force they could obtain code and join meeting
2. The camera function in Zoom has vulnerability that could allow someone to easily hack in and project inappropriate images during a meeting – called Zoom bombing and currently very popular with people with time on their hands
3. Default settings for Zoom do not encourage passwords to be set for meetings
4. Device data sent from Zoom to Facebook – this supposedly has now stopped as this was leaked out to public
5. It does not use end to end encryption even though its website says it does
6. There is an attendee tracking feature where host can track whether participant has Zoom live on their screen or just dormant in the background

Some mitigation for its use is:

- Remember to set a password on the meeting for both the web meeting and for users who phone in (there are settings for this) – you could ask organisers to do this
- Don't broadcast or screengrab the meeting like they did in the cabinet meeting as it exposes the meeting ID and usernames of the attendees (meeting passwords can be bruteforced)
- Be clear who you are inviting, who knows who the iPhone user was, and hopefully they do know who that was – if you are not setting up but participating you might just want to confirm who is in the meeting
- Don't share personal identifiable information or sensitive information, Zoom may clear a few things up in the future around compliance and controls hopefully.

Remember any video conferencing concerning school related business should be done through Microsoft Teams.

Communication – To support the challenges of distance learning the following has been agreed:

Staff will be contactable between the hours of 8.30am and 3.30pm via email. However, staff may not be able to respond straightaway as they will be planning, setting work or delivering feedback where appropriate. As a result, any response may not be received that working day, but staff will endeavour to contact you as soon as possible.

Staff will communicate with students through the messaging service within Show my Homework or via school email.

The expectation for communication regarding distance learning with parents can be found in Appendix A.

This supports a system of checks to ensure pupils can access the work and checks on pupil welfare.

Vulnerable pupils have been identified and have regular contact via a key worker. The outcomes of these are monitored by the DSL.

The established systems ensure that the schools child protection policy continues to operate remotely.

All school staff should be familiar with the school's Safeguarding and Child Protection Policy.

Scott Wycherley
Deputy Headteacher
April 2020

Monitoring Student Work and Engagement

Teachers

- Teachers should be setting work as per timetable. However, be mindful of the work set.
- Do not ask for submit by Show My Homework for every piece of work. This will be unmanageable for you and for the students.
- Set one piece of assessed work every 6-9 pieces. You may wish to set on-line knowledge quizzes that self-mark more frequently. *Remember you are giving general feedback and not marking to the same extent.*

Monitoring Student Engagement – Subject teachers

Teachers check students have logged on and have looked at work

On the task that you have set – Click on "insights"

Then click on reminders – you can then see if a student has viewed the task.

What to do if student has not looked at the work?

Go to manage class – Assess

Send the student a reminder in the comments section or email student

Ask if they are having issues with the work?

Next time you set work for this class repeat above steps. If they fail to check/submit work despite above reminder – then email or phone home.

Ask parents if students are finding it difficult to log or having difficulty accessing work. Record contact with home on spreadsheet your initials and date

If SEN student is struggling email Shirley to put you in contact with their key TA who will be contacting home.

Spreadsheet can be found here:

L:\Staff Resources\Staff Info\Distance Learning\Monitoring Distance Learning

Before contacting home please check contact with home spreadsheet

Note students highlighted in yellow already have a member of staff in regular contact (see tab for vulnerable and SEN)

Contact the key worker with your concerns.

> Following your contact with home – if student is still not working
>
> Then refer to your Head of Department
>
> Head of Department contacts home.
>
> Head of department email to Head of Year to inform

Heads of Year Monitoring

- Heads of Year to monitor year group engagement weekly. Choose a day and email teaching staff to state which day you will be monitoring.
- Be mindful when making contact with parents that the last logged in time may not be accurate. If they stay logged in on a mobile phone and do not log out then this may not be updated, so phrase concerns carefully
- Monitor students logging onto Show My Homework via reports, user activity report – then filter by year group. Check PP students and SEN students using filters. Also check vulnerable students log in too.
- Focus on top ten students most likely to disengage and keep in regular contact with parents.
- Individual subject concerns – make sure that the teaching staff have followed the above steps. It is the teacher and the departments job to chase work.

> Head of Year
>
> Weekly – check user activity report/submissions report
>
> If student has not logged on in the last week – send the student a prompt via Show My Homework

> Following week
>
> If the student is still not logged in – please contact home.
>
> Check all is OK.
>
> If next week still not engaging – speak to parents again