# Idsall School
# Remote Learning Policy

## Sponsorship & Review

### 1 Sponsor

Mr M Bishton – Deputy Headteacher

### 2 Ratified

March 2022

### 3 Next Review Date

March 2023

## Contents



---

## 1. Aims

This remote learning policy for staff aims to:

- Ensure consistency in the school's approach to remote learning
- Set out expectations for all members of the school community with regards to remote learning
- Provide appropriate guidelines for data protection

## 2. Roles and responsibilities

### 2.1 Teachers

Teachers would normally be expected to work within the school building. However, if directed by the Headteacher to work from home for any reason, teachers must be available between 8.40am and 3.00pm. If they're unable to work for any reason during this time, for example, due to sickness or caring for a dependent, they should report this to the Headteacher / Cover Supervisor (CLE).

Teachers are responsible for:

- Setting work:
    - Work should be set for each of a teacher's timetabled classes. (Where classes are shared, responsibility for setting the work should be split proportionately.)
    - The amount of work set, should equate to the number of timetabled teaching hours per week.
    - In the event of whole groups of students or the whole school community working remotely, there is an expectation that a minimum of 60% of lessons on the timetable for each subject should be live and 40% consisting of work set by the class teacher on Satchel One.
    - The work should be set via Satchel One, with any materials needed being attached / linked to the instructions for each task. Work may be varied in nature and can include, but is not exclusive to, note taking, task completion, use of online packages such as Active Learn or Kerboodle, online quizzes, websites such as BBC Bitesize, etc.
    - Teachers should coordinate with other teachers to ensure consistency across the year/subject and to make sure students with limited access to devices can still complete the work.

- Providing feedback on work:
    - Completed work can be uploaded for teachers via Satchel One or shared as a document via OneDrive. Quizzes set on Satchel One are self-marking.
    - Feedback should be given formally on key assessment pieces as defined in the schemes of learning. If using Microsoft (MS) Teams, feedback can be provided through the use of the assignments feature that gives instant feedback to students once marked.
    - If students complete a unit of work remotely, an assessment should be set online for students to complete at home. Assignments in Teams should be used to give formal feedback alongside existing packages used by departments that can be used to give detailed feedback.
- Keeping in touch with students and parents:
    - If contacting home via telephone, staff should make contact from school, if in the building at the time. If using personal phones, staff should ensure that personal numbers are withheld.
    - Tutors contacting home for pastoral purposes should ensure that any issues are passed on to the appropriate member of staff, where appropriate, and notes recorded on CPOMS. (Teaching and learning issues – refer to class teacher / head of subject, pastoral issues – refer to head of year, safeguarding issues – refer to designated safeguarding lead (DSL) immediately).
    - Emails from students / parents should be responded to from a school email address within normal working hours. A response should be sent within one working day of receipt of email; this may take the form of a 'holding email' if necessary.
    - Emails to students should only be to the student's school email address. Messages can also be sent to students via Satchel One.
- Attending virtual meetings with staff, parents and students:
    - These should only take place within the school's working hours.
    - MS Teams must be used for virtual meetings.
    - Staff should take care in choosing the location from which they are meeting, ensuring that there is nothing inappropriate in the background and that they will not be disturbed during the meeting by someone who does not work for the school.
    - A note of the time of any virtual meeting with students / parents should be made on CPOMS (if not part of the school timetable or calendar of events e.g. parents evenings, options evenings) along with any notes from the meeting which are deemed necessary.
    - Any concerns arising from a virtual meeting with students / parents should be passed on to the appropriate member of staff, where appropriate, and notes recorded on CPOMS. . (Teaching and learning issues – refer to class teacher / head of subject, pastoral issues – refer to head of year, safeguarding issues – refer to designated safeguarding lead (DSL) immediately).
- Online teaching:
    - Lessons should only take place within the school's working hours and should last no longer than the allocated time on the timetable.
    - MS Teams must be used for online live teaching. No other platform should be used.

- Staff should take care in choosing the location from which they are teaching, ensuring that there is nothing inappropriate in the background and that they will not be disturbed during the lesson by someone who does not work for the school. (The 'Blur Background' function can be used on MS Teams if needed.)
- Notice of the lesson should be through an email notification to students on the school email system. This will then sit in their outlook calendar to join the lessons.
- Cameras and microphones are turned off as a Teams default setting on our school network. Students can be prompted by the teacher to turn on their microphone to answer questions where appropriate.

## 2.2 Teaching assistants

Teaching assistants must be available between 9.05am and 3.00pm on their allocated rota days. If they're unable to work for any reason during this time, for example, due to sickness or caring for a dependent, they should report this using the absence procedure - currently contact Headteacher and inform Support for Learning Coordinator, L. Barrass.

Teaching assistants will be timetabled to individual classes in school by J Laing – KS 4 Inclusion Base Manager.

Teaching assistants are responsible for providing additional support to identified students led by the subject teacher:

**SEND students in school:**

- In-class support for identified SEND students – principally those with EHCPs along with students identified on the SEND list at SEN Support where appropriate.

**SEND students working at home:**

- Weekly telephone calls to check on well-being and any issues of work completion being set for Home Learning to be made by teaching assistants to EHCP students.
- Record of telephone calls to be logged on CPOMS and any issues or concerns to be raised with L Barrass - Support for Learning Coordinator and/or C. Cork, Assistant Headteacher – Pupil Support and Inclusion.

- Teaching assistants also prepare notes/modified materials for specific needs as required by the teacher.
- Teaching assistants as required to sign in to live lessons to support EHCP students as directed by the SEND team.

## 2.3 Subject leads

Alongside their teaching responsibilities, as outlined above, subject leads are responsible for:

- Monitoring the work set remotely for their subject area. (Amount / timing etc.) Including the timings and frequency of live lessons.
- Working with teachers teaching their subject to make sure work set is appropriate and consistent.
- Working with other subject leads and senior leaders to make sure work set across subjects is appropriate and consistent, and deadlines are being set an appropriate distance away from each other.
- Monitoring the work set by teachers in their subject – explain how they'll do this, such as through regular meetings with teachers or by reviewing work set.
- Alerting teachers to resources they can use to teach their subject.

- Adapting the curriculum as appropriate for remote learning.
- Ensuring that timely, appropriate assessments are set after a unit of work.

### 2.4 Senior leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

- Coordinating the remote learning approach across the school (DCA / MBI will liaise regarding this).
- Monitoring the effectiveness of remote learning, through regular meetings with subject leaders, reviewing work set or reaching out for feedback from students and parents.
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations.

### 2.5 Designated safeguarding lead

The DSL is C Cork, Assistant Headteacher

The other safeguarding leads are:

Mrs J Reeve (Deputy DSL)

Mr C Bailey

Mr A Baldwin

Ms D Campbell

Mrs H Lynn

Ms M King (Headteacher)

The Child Protection Policy has been reviewed and updated and is available on the school website.

### 2.6 IT staff

IT staff are responsible for:

- Fixing issues with systems used to set and collect work
- Helping staff and parents with any technical issues they're experiencing
- Reviewing the security of systems and flagging any data protection breaches to the data protection officer
- Assisting students and parents with accessing the internet or devices

### 2.7 Students and parents

Staff can expect students to:

- Be contactable during the school day – although they may not always be in front of a device the entire time
- Complete work to the deadline set by teachers
- Seek help if they need it, from teachers or teaching assistants
- Alert teachers if they're not able to complete work or have issues with access
- Behave appropriately during online lessons.  Inappropriate behaviour during a video lesson will result in the student being removed from the lesson and potentially banned from participating in future online lessons

- Sign in to live lessons as invited by the class teacher

Staff can expect parents to:

- Make the school aware if their child is sick or otherwise can't complete work
- Seek help from the school regarding remote learning, if they need it

### 2.8 Trustees

The trustees are responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible
- Ensuring appropriate security policies are in place, for both data protection and safeguarding reasons

## 3. Who to contact

If staff have any questions or concerns, they should contact the following individuals:

- Issues in setting work – talk to the relevant subject lead
- Issues with behaviour – talk to the relevant head of year
- Issues with IT – talk to IT staff
- Issues with their own workload or wellbeing – talk to their line manager
- Concerns about data protection – talk to DCA
- Concerns about safeguarding – talk to the DSL

## 4. Data protection

**Everyone *in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.***

**Where to get advice**

The Information Asset Owners manage and address risks to the information and understand:

- what information is held, for how long and for what purpose
- that data can only be used in ways consistent with the purpose/s for which it was obtained, and that data is disclosed only in ways consistent with that purpose
- how information has been amended or added to over time
- who has access to protected data and why

All staff must always follow the GDPR – Data Protection Policy – a full copy is available in the Policies folder on the school network. For convenience, a summary of relevant practical steps is included in the sections below.

### 4.1 Keep data safe and secure

When accessing personal data, all staff members will ***keep data safe and secure:***

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

a. All paper-based material containing sensitive personal data must be held in lockable storage, whether on or off site. (ALL staff)

b. Idsall School designates the Deputy Headteacher, Ms D Campbell and the Network Manager, Mr A Groucutt (AG) as the persons with responsibility for the security of IT systems

c. The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. (AG – Network Manager)

d. All users will use strong passwords which must be changed regularly, every 100 days. User passwords must never be shared. (AG – Network Manager)

e. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). (ALL staff)

f. As a backup 'auto lock' will be enabled on all computers. (AG – Network Manager)

g. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. (AG – Network Manager)

h. Personal data can only be stored on school equipment. Private equipment (i.e. owned by the users, including personal cloud storage accounts and personal email accounts) must not be used for the storage of personal data. (ALL staff)

i. Ensure that no unauthorised person can access data from computers that are no longer in use or subject to change of use. This will normally require the removal of all storage media from the device and safe disposal of any data stored on that media. (AG – Network Manager)

j. The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (AG – Network Manager)

k. The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data. (AG – Network Manager)

## 4.2 Sharing personal data

Idsall School may need to access personal information, such as email addresses as part of the remote learning system. Such collection of personal data applies to our functions as a school and doesn't require explicit permissions.

While this may be necessary, individual members of staff are reminded that they should not collect and/or share personal data online as part of their 'online teaching and learning' activity. Any data required to carry out online teaching and learning will be collected and managed centrally by the Network Manager.

## 4.3 Secure transfer of data and access out of school

Idsall School recognises that personal data may be accessed by users out of school; or transferred to the LA or other agencies. In these circumstances:

a. Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and only when the criteria (b) and (c), below are met. (ALL staff)

b. When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform. (ALL staff)

**NOTE:**

VPN is available to use via staff laptops.

Ericom Remote Access is available to use from all other devices.

a. If secure remote access is not possible, personal data can only be stored on your "staff laptop". (ALL staff):

b. The use of USB stick, CD/DVD or any other removable media is not permissible for the transfer of personal data outside of school. (This also applies to examination board requirements.)

c. Users must take particular care that computers (staff laptops) which contain personal data must not be accessed by other users (e.g. family members) when out of school. (ALL staff)

d. If staff take home paper-based materials containing personal data (including exercise books, assessments, tests or exam scripts) these documents must NOT be left in a vehicle overnight.

e. Staff will be made aware of all practical measures to ensure the security of personal data, annually and through 'new staff' induction procedures. (DCA – Data Protection Lead)

f. SIMS access will only be given to persons on contract to Idsall School or persons where an SLA exists requiring them to have SIMS access.

g. Trainee and associate teachers working and training temporarily at Idsall School will, as part of their induction process, be required to encrypt and password protect any removable media device that they intend to use whilst on placement at Idsall School. They must seek approval from the Network Manager. At the end of their placement, they must present their removable media device to the Network Manager in order to ascertain and ensure all and any personal data has been removed from their device.

Sending information via email is by default not secure just like sending mail in the postal system the mail can be intercepted and read by anyone:

h. email attachments that contain personal data must be password protected and encrypted first before sending them, but then providing the recipient a password via separate communication channel, for example, a phone call.

## 4.4 Data Breaches

### What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen

- alteration of personal data without permission and
- loss of availability of personal data.

***If a member of staff considers that a breach of personal data has occurred, they will inform*** Ms D Campbell / Mrs V Hulme / Mr A Groucutt ***and complete sections 1 – 4 of the Personal Data – Breach Record within 24 hours.*** (ALL staff)

## 5. Safeguarding

The Child Protection Policy is reviewed and updated annually – it has been further updated in light of current situation and is available on the school website.

## 6. Monitoring arrangements

This policy will be reviewed every 12 months (or sooner if deemed necessary) by MBI. At every review, it will be approved by Michelle King and / or the Trustees.

## 7. Links with other policies

This policy is linked to our:

- Behaviour policy
- Child protection policy
- Data protection policy and privacy notices
- ICT and internet acceptable use policy
- E-safety policy