Charlton Park Academy
Online Safety and ICT Acceptable Use Policy

Date reviewed: October 2025
Next review date: October 2026

1. Rationale

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is the Chair of Governors.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet Appendix 4
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing body

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet Appendix 3, and ensuring that students follow the school's terms on acceptable use Appendix 2
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet Appendix 2
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? – UK Safer Internet Centre
    - Hot topics – Childnet International
    - Parent resource sheet – Childnet International
    - Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum. The Health Education curriculum includes online safety for all students at Charlton Park Academy. Additional guidance on relationships education, relationships and sex education (RSE) and health education.

It is a legal requirement for CPA to teach `Relationships and sex education and health education` this is the case for all secondary schools

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant and in dedicated tutor time and focus sessions.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE/TEAMS). This policy will also be shared with parents. Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of School and/or Principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (RSE/HE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 16 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

  * Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Use of Computers

- The use of academy computers/IT will be permitted only for purposes directed by the academy and not for personal use. Everyone will treat all school ICT equipment with respect and care.
- Users are not permitted to access and amend another user's work without permission.
- All PC's connected to the Internet will be protected by anti-virus software which is kept up to date. All software is monitored through the ICT department and will be checked before approval and loaded onto our network. Our network has a backup system in place.

- No files should be brought in from home and loaded onto the system without permission of a teacher.
- Staff should not create or keep any personal files on school systems or computers as these are for school business use only.
- No files created at school by any staff, stored or kept on a school computer or system are permitted to be transferred or exported to a pen drive or any digital media to any off-site location. Files containing pupil data must be encrypted or require password protection.
- The data protection policy and Data Protection Act 1998 advice must be followed.
- The school reserves the right to look, review and monitor all or any files on the school systems including text, graphics and emails. Failure to follow procedures can lead to disciplinary action.
- The school reserves the right to deny access to the schools computer systems.

8. Internet Access

- The school provides Internet access for educational purposes and should only be used by staff, students and members of the community for these purposes.
- The school connects to the Internet via a filtered service. Students cannot use computers without filtered access. The Mac computers have a lower level of filtering to enable e safety teaching of social networking and students will always be supervised when using these computers.
- No student, member of staff or community user is permitted to access material that is illegal or potentially offensive using the school system. All users should be aware that usage is monitored centrally, and any misuse will be reported and appropriate action will be taken.
- A programme of e safety is continually taught to our students and they will be fully aware not to post any personal information about themselves or others.
- Students will only download files with permission and ensure they are from a trusted source. Files will always be appropriate and for school use and will not breach copyright infringement.
- Parents/Carers are asked to sign the responsible ICT and Internet use policy indicating that they understand the issues and give consent for their child to use the Internet. Likewise, those students who are able will also sign an agreement on acceptable use.

9. Social Networking sites (including Facebook, Twitter, Flicker, Audioboo, blogs and Instagram)

The academy uses a range of networking and media sites and intends to develop and continue to grow the ways we interact with our wider community along with ensuring we protect our whole community (students, staff and families) from any misuse. The primary use for these sites is to share and celebrate the achievements and activities of the Academy along with raising disability awareness and positive attitudes within our local and wider community. Therefore:

- All media publications and use of the schools social networking sites such as Twitter are monitored and managed through our school digital media and communications officer and ICT lead.
- The Academy site is set up so that staff do not use their own personal accounts. We are aware that it is very easy to link to personal information on many of these sites. Individual teachers who hold an interest in using our Academy sites like Twitter will be given login details and must keep login information securely.

- It is the responsibility of the individual posting on our sites to check permissions of students and to ensure no full names are used and their identity is protected. They should also ensure material doesn't breach copyright and data protection. For more information on copyright law see: http://www.legislation.gov.uk/ukpga/1988/48/contents
- Staff will not allow students to become 'friends/contacts 'to their own networking sites. If when teaching students how to use such sites a demo is needed, then a teaching site can be set up.
- Staff should also be cautious when adding ex-students to 'friends/contacts' on sites and maintaining contact.
- Staff are not to share any Academy information or images on their own sites and these should not be accessed during Academy time.

10. Publishing on the Internet and Academy Website

- Parents/Carers will sign an annual consent form on permission to use student images on our website and other media sites. Likewise, with the use of video.
- Students are given the opportunity to publish projects, artwork or schoolwork on the web.
- We will never use full names on our school website and every precaution will be taken to limit identification of students.
- All publications and use of the schools social networking sites like Twitter are monitored through our school digital media and communications officer.

11. Logins and Passwords

- No one is given access to our network without approval from Admin and a procedure for logins is in place. Usernames for the domain are set using the following naming convention: First initial + surname, e.g. "jsmith"
- Because of the various accessibility needs of our students we have a standard password to access the network. There may be times when we feel it's appropriate to change an individual's login. No students are permitted to access anyone else's login without their permission.
- Everyone requires passwords and we all have responsibility to keep these safe, change the password regularly and never give these details to anyone else. Everyone also needs to ensure they log out after use and close the Internet browser window.
- Everyone is required to change their password regularly and our computer system will lock after a short period of time when not in use.
- RIX Wiki passwords are to be kept private and are centrally stored with. Class tutors may also have a copy which is kept privately.
- Password information for any of our internet sites will be the responsibility of staff to keep confidentially.

12. Administrative systems

- All personal details of students and staff are kept on a secure administrative system and access is only given to key staff as monitored by the administration leader.
- All staff are aware of this sensitive and privileged information and hold professional standards to ensure this information is held and treated confidentially.

13. Email

- Staff will not give out their personal email address to students.

- The school email is primarily for school use and should not be used to send unrelated material. Anyone found to be misusing their email addresses e.g. sending offensive materials could result in disciplinary action.
- Students are taught not to disclose or publicize personal or confidential information for example home address, telephone numbers, name and location of school without their teacher's permission.
- All incoming and outgoing emails are checked for inappropriate content or subject lines and any such emails will be quarantined and the system manager is notified. Likewise, for any emails containing a virus.
- Any spam, viruses, spyware or suspicious emails are to be reported to the IT department.
- All accounts on the school domain are automatically set up with a corresponding email address. Students are also encouraged to use their email under staff supervision at appropriate times.

14. Mobile Technologies

- Mobile phones and other portable devices will not be used during lessons or formal school times unless under the direction of a member of staff. If students bring in mobile devices from home, they will be securely held until the end of the day unless this part of an agreed activity with the teacher.
- Parents/Carers and students should be aware that Charlton Park Academy cannot be made accountable for personal equipment borough from home and students do this at their own risk.
- At Charlton Park Academy we are open to new and emerging technologies as we are aware of the accessibility and huge potential in teaching and learning. Risk assessment and protocol will be developed along with any use of new equipment or Internet resource.
- Students in Mulberry Tree House can access to their own devices but will be monitored by staff. The students have access to store equipment securely if needed.

15. Individual Wiki Sites

- All students are given their own individual wiki site. These are secure sites which are provided and administered by The Rix Research and Media Centre. It is our intention that these sites will be lifelong tools for our students and that ownership will be with the young person and or with their family.
- We will support students and families by monitoring the Wikis and providing feedback and support to ensure they are used primarily as a student self-advocacy tool.
- RIX Wiki passwords are to be kept private and are centrally stored. Class tutors may also have a copy which is kept privately.

16. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

17. Student and Staff Agreement

Students will be made aware that if they deliberately break these rules, they may not be able to use the Internet or computers for a period of time and further action may be taken. Also, all students have a responsibility to report any misuse or any concerns they might have.

All staff and students should annually sign an acceptable use agreement and if they use school IT equipment are deemed in practice to be held to have implicitly agreed to accept the Safety and ICT Acceptable Use Policy and agreement with all of the terms.

18. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on `My Concern`.

This policy will be reviewed every year by the ICT Lead and DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

19. Helpful Websites for Parents

http://kids.getnetwise.org/safetyguide/technology/socialnetworking
http://www.childnet-int.org/blogsafety/parents.html
http://www.wiredsafety.org/safety/email_safety/index.html
http://www.childnet-int.org/sorted/filesharing.aspx
http://computer.howstuffworks.com/internet-infrastructure.htm
http://www.privacyrights.org/fs/fs17-it.htm
http://www.microsoft.com/protect/yourself/email/imsafety.mspx
http://www.google.co.uk/familysafety/
http://www.thinkuknow.co.uk/
http://www.bbc.co.uk/cbbc/help/web/staysafe

Anyone requiring any extra information, support or training please contact the ICT Department.

Addendum I: Undertaking Remote Teaching and Online Communication Safely

1. Introduction
In England, the Department for Education (DfE) has no expectation that teachers should livestream or pre-record lessons. Charlton Park academy will consider the approaches that best suit the needs of its students and staff (DfE, 2020).

If lessons/communication is recorded or livestreamed via an online platform, CPA will assess any risks and take appropriate actions to minimise harm (**see Appendix 1 – Recording**).

2. Where is the recording taking place?
Teachers/staff must use a neutral area where nothing personal or inappropriate can be seen or heard in the background.

3. Which platform will you be used?
Teachers/staff will ensure the platform used is suitable for the children's/family's ICT knowledge and ability, e.g. Set up school accounts for any online platforms used (not using teachers' personal accounts). Privacy settings must be checked.

4. Consent
Parents, carers and children should understand the benefits and risks of online lessons and getting written consent for children to be involved (**see Appendix 2 - Consent Form**).

5. Contacting Children at Home
When CPA is fully or partially closed, staff might need to contact children individually. Staff should only contact children during normal school hours, or at times agreed by the school leadership team (DfE, 2020).

Staff must refer to CPA's Code of Conduct and be clear how the academy expects them to behave.

Any one-to-one sessions, for example pastoral care meetings, must be risk assessed and approved by the Senior Leadership Team (DfE, 2020). Staff must know what safeguarding measures to take if they are having a one-to-one conversation with a child – see link below:

One-to-one contact

Parents' or carers' email addresses or phone numbers must be used to communicate with children, unless this poses a safeguarding risk. School accounts must be used to communicate via email or online platforms, never personal accounts.

Phone calls must be made from a blocked number, so personal contact details are not visible unless with a work phone.

Staff members accessing families' contact details at home must ensure they comply with the Data Protection Act 2018.

6. Child Protection Concerns

All staff must refer to CPA's Safeguarding and Child Protection Policy and Procedures.

Staff must contact the DSL or deputy if they have any concerns about a child. This may be because:

- a staff member sees or hears something worrying during an online lesson
- a child discloses abuse during a phone call or via email.

The nominated lead should keep a note of any contact numbers they may need while the school is closed, for example children's social care and the local police.

NOTE: The NSPCC helpline can be contacted for advice if there are worried about a child's wellbeing.

Tel. 0808 800 5000
Email: help@nspcc.org.uk

7. Online Safety

Children and young people are likely to spend more time online due to social distancing. The benefits and risks of the online world should be discussed regularly with them and they should be given the space to ask questions and talk about anything that worries them.

8. Mental Health and Wellbeing

Children and young people may be worried about the impact of coronavirus, social distancing or self-isolation. Those who already have mental health difficulties such as anxiety might be finding things particularly tough. Where appropriate, they should be talked to about what's happening, checking how they are feeling and keeping them as well informed as possible.

Where appropriate, children and young people should be told where they can go if they are worried about anything or need to talk to someone while school is closed.

Childline provides a range of online tools that young people might find helpful: information about coronavirus:

- Calm Zone – activities to help let go of stress
- Games to help take your mind off things
- Information and advice on a range of topics including feelings, relationships, family and schools
- Peer support message boards
- Childline Kids - website for under 12s.

Childline can also give confidential help and advice. Calls to 0800 1111 are free or children can get support online.

Addendum II: Flow Chart for Communication with Parents and Carers

This guidance is designed for all communication with Parents and Carers and includes Covid-19 Welfare Check and/or when a student is absent from school (after the third day of absence). This guidance does not replace home school contact books.

1. Class Teacher

Contact the parent/carer where possible using `Teams`. We have sent letters home to audit IT access and to provide equipment and WIFI as required.

(If this is not possible because the parent/carer does not have ICT access, please email your middle leader. This will enable us to remediate the ICT issues and telephone as an interim measure).

2. During the `Teams` Meeting

Please ensure that you: Follow the guidelines as set out in **Addendum I: Undertaking Remote Teaching and Online Communication Safely.**

3. Log all communication on `My Concern`

Follow the steps below.

Step 1-8 required for the first communication log.

1. Log on to `My Concern`.
2. Report a concern. Student Name: _____.
3. Concern Summary: Covid -19 Welfare check communication with Parents & Carers.
4. Send concern: Designated Safeguarding Leads.
5. Details of concern: Use this box to summarise the conversation and to highlight any concerns with well-being, any issues that might arise in the conversation, ability to access and engage with 'Remote/ Home Learning. This is also a great opportunity to record positive feedback to discuss strategies/learning activities that are working well.
6. Date and time: Populate accordingly. This helps to provide a chronology of communication dates and times.
7. Location of incident: Remote/Home Learning taking place in student home.
8. Action taken: Concerns if any escalated to middle leader, DSLs sent notifications (step 4).

4. Weekly communication (If absence continues past 5 days)

1. Log on to `My Concern`. Search student name. Click on the first concern raised (will have date and identification number)
2. Click on the tab named Chronology. Three tabs appear below, click on `Add concern update`
3. Concern update type: scroll sown to COVID-19 welfare check and click.
4. Update occurred at different time to recording, populate accordingly, this helps to provide a chronology of communication dates and times.
5. Update text box: Use this box to summarise the conversation and to highlight any concerns with well-being, any issues that might arise in the conversation, ability to access and engage with 'Remote/ Home Learning.
6. Add update. Click on this box.

7. ***Any issues or concerns should be escalated to your middle leader and senior leaders.**

Appendix 1 Recording
If lessons/contact are to be recorded:

Consent in writing must be given before making the recording.

In addition:
- The recording will only ever be used for the purpose of tuition for the individual pupil, and may include voice and images
- The recording will be kept as part of the student's digital records.
- CPA guarantees that the recording will only ever be shared with the pupil (if an adult) or the parents/guardians.
- The recordings will be disposed of securely at the end of the retention period of three years, if appropriate.
- That CPA will securely delete and dispose of recordings as quickly as possible if students or their parents withdraw consent.
- A Data Protection Impact Assessment (DPIA), as outlined below, must be carried out for those using the system (**see Appendix III for template**).

A DPIA is a process to help identify and minimise data protection risks.

A DPIA must be undertaken if an action is likely to result in a high risk to individuals. This includes some specified types of projects.

The DPIA must:
- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

.

To assess the level of risk, the likelihood and the severity of any impact on individuals must be considered. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

Appendix 2

Consent Form (this will also be made available digitally on our website)

Parental/Carer Permission for taking part in online teaching/communication sessions between Charlton Park Academy and CENMAC staff and students/home.

STUDENT'S NAME: .....

PARENT/CARER NAME: ……

I hereby give consent for my child to take part in an online teaching/communication session with Charlton Park Academy or CENMAC staff.

I will agree the most appropriate time within a normal teaching day and appropriate space.

I hereby give permission for my child's online session to be recorded part of the ongoing record of these teaching and or communication sessions. The staff member will inform the parent/carer prior to the session if it is being recorded.

I understand that this recording is then held securely and inline with data protection policy of the Academy/CENMAC service.

I am aware that the recordings will be disposed of securely at the end of the retention period.

That CPA will securely delete and dispose of recordings as quickly as possible if students or their parents withdraw consent

SIGNED: .....

PLEASE PRINT NAME: .....

DATE: .....

Appendix 3 KS2, KS3 and KS4 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4 Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of students without checking with teachers first • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5

Data Protection Impact Assessment

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA