Data Protection Policy and Privacy Notice

<table>
<thead>
<tr>
<th>Document title</th>
<th>Data Protection Policy and Privacy Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version number</td>
<td>1.1</td>
</tr>
<tr>
<td>Policy status</td>
<td>Approved</td>
</tr>
<tr>
<td>Date of issue</td>
<td>July 2020</td>
</tr>
<tr>
<td>Date to be revised</td>
<td>July 2022</td>
</tr>
<tr>
<td>Owner</td>
<td>Sophie Hanson</td>
</tr>
<tr>
<td>Author</td>
<td>ESCC</td>
</tr>
</tbody>
</table>

Revision log (last 5 changes)

<table>
<thead>
<tr>
<th>Date</th>
<th>Version No</th>
<th>Brief detail of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2020</td>
<td></td>
<td>Updates to 'Roles &amp; Responsibility, Data Protection by Design and Other data protection rights’</td>
</tr>
</tbody>
</table>
# Contents

1. Aims ............................................................................................................................... 1
2. Legislation and guidance ................................................................................................. 1
3. Definitions ........................................................................................................................ 1
4. The data controller ............................................................................................................ 2
5. Roles and responsibilities ................................................................................................. 2
6. Data protection principles .................................................................................................. 3
7. Collecting personal data .................................................................................................... 4
8. Sharing personal data ........................................................................................................ 4
9. Subject access requests and other rights of individuals ..................................................... 5
10. Parental requests to see the educational record ............................................................... 9
11. Biometric recognition systems ......................................................................................... 9
12. CCTV ................................................................................................................................ 10
13. Photographs and videos ................................................................................................. 10
14. Data protection by design and default ............................................................................. 11
15. Data security and storage of records .............................................................................. 11
16. Disposal of records ........................................................................................................ 12
17. Personal data breaches .................................................................................................... 12
18. Training ........................................................................................................................... 12
19. Monitoring arrangements ................................................................................................. 12
20. Links with other policies .................................................................................................. 13
Appendix 1: Uplands Data Breach Management Process .................................................. 14
Appendix 2 Third Party Requests for Information ............................................................... 17
1. Aims
Our College aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR and the ICO’s code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO’s code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child’s educational record.

3. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Any information relating to an identified, or identifiable, individual. This may include the individual’s:</td>
</tr>
<tr>
<td></td>
<td>● Name (including initials)</td>
</tr>
<tr>
<td></td>
<td>● Identification number</td>
</tr>
<tr>
<td></td>
<td>● Location data</td>
</tr>
<tr>
<td></td>
<td>● Online identifier, such as a username</td>
</tr>
<tr>
<td></td>
<td>It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.</td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</td>
</tr>
<tr>
<td></td>
<td>● Racial or ethnic origin</td>
</tr>
<tr>
<td></td>
<td>● Political opinions</td>
</tr>
</tbody>
</table>
### Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

### Data subject

The identified or identifiable individual whose personal data is held or processed.

### Data controller

A person or organisation that determines the purposes and the means of processing of personal data.

### Data processor

A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

---

### 4. The data controller

Our College processes personal information relating to students, staff, governors and visitors, and, therefore, is a data controller. Our College delegates the responsibility of data controller to the Director of Finance, Business, Premises, and Administration.

The College is registered as a data controller with the Information Commissioner’s Office and renews this registration annually.

### 5. Roles and responsibilities

All employees, Governors and any other individual handling personal information on behalf of the College have a responsibility to ensure that they comply with Data Protection legislation and the College’s policies.

The College ensures that all staff who are involved in processing personal data complete the College’s mandatory data protection training.

Staff who do not comply with this policy may face disciplinary action.
5.2 Data protection officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Board and, where relevant, report to the board their advice and recommendations on the College data protection issues.

The DPO is also the first point of contact for individuals whose data the College processes, and for the ICO.

Full details of the DPO’s responsibilities are set out in their job description.

Our DPO is Mr Peter Questier and is contactable by telephone on 01273 337610 or by email: CS.DPA@eastsussex.gov.uk

5.4 All staff
Staff are responsible for:

● Collecting, storing and processing any personal data in accordance with this policy
● Informing the College of any changes to their personal data, such as a change of address
● Contacting the DPO in the following circumstances:
  o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  o If they have any concerns that this policy is not being followed
  o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  o If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  o If there has been a data breach
  o Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  o If they need help with any contracts or sharing personal data with third parties

6. Data protection principles
The GDPR is based on data protection principles that our College must comply with. The principles say that personal data must be:

● Processed lawfully, fairly and in a transparent manner
● Collected for specified, explicit and legitimate purposes
● Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
● Accurate and, where necessary, kept up to date
7. Collecting personal data

7.1 Lawfulness, fairness and transparency
We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

● The data needs to be processed so that the College can fulfil a contract with the individual, or the individual has asked the College to take specific steps before entering into a contract
● The data needs to be processed so that the College can comply with a legal obligation
● The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life
● The data needs to be processed so that the College, as a public authority, can perform a task in the public interest, and carry out its official functions
● The data needs to be processed for the legitimate interests of the College or a third party (provided the individual’s rights and freedoms are not overridden)
● The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the College’s Record Retention Schedule.

8. Sharing personal data
We will not normally share personal data with anyone else, but may do so where:
• There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
• We need to liaise with other agencies – we will seek consent as necessary before doing this
• Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
  o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
• The prevention or detection of crime and/or fraud
• The apprehension or prosecution of offenders
• The assessment or collection of tax owed to HMRC
• In connection with legal proceedings
• Where the disclosure is required to satisfy our safeguarding obligations
• Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests
Individuals have a right to make a ‘subject access request’ to gain access to personal information that the College holds about them. This includes:
• Confirmation that their personal data is being processed
• Access to a copy of the data
• The purposes of the data processing
• The categories of personal data concerned
• Who the data has been, or will be, shared with
• How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
• The source of the data, if not the individual
• Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our College may not be granted without the express permission of the pupil. This is not a rule and a pupil’s ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests
When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child’s best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.
9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Right of erasure

This right allows individuals to request that their personal data is deleted where there is no justification for its continued use. It only applies, however, when:

1. The data is no longer necessary for the reason(s) for which it was originally collected
2. The data subject provided consent for the College to process their data but has subsequently withdrawn this consent
3. That data subject has objected to the College processing their data and there are no overriding grounds for continuing to process it
4. The data was processed in breach of the GDPR i.e. it was unlawfully processed
5. There is a legal requirement to erase the data
6. The data was collected with parental consent when the data subject was a child and they no longer wish for their data to be held

The College will decline a request for erasure:

1. When we have a legal obligation or it is part of our official authority to process the data
2. For public health reasons
3. For certain archiving activities
4. When we need the data in connection with a legal claim

Right to rectification
If data subjects believe that any of the personal data the College holds about them is inaccurate or incomplete they are entitled to ask for it to be rectified. This will be looked at in the context of why the College is processing the information any necessary steps will be taken to supplement the information held in order to make it complete.

Right to restriction
In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the College processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data, but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn’t apply if:

1. The processing is necessary for the College in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

Right to portability
Data subjects have a right to request that their data be transferred electronically to another organisation.

This only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

Right to object
Data subjects have the right to object to their information being processed in the following circumstances:

- If the College has decided that processing is necessary, either to
  a) perform a task carried out in the public interest or
  b) as part of the College’s official authority or legitimate interest and the data subject feels this is not applicable.
  Information about why the College is processing information (the legal justification) can be found in the College’s privacy notice.
- If the College retains information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.
Data subjects also have a right to object to their data being used for direct marketing purposes at any time and the College will cease processing for this purpose if an objection is raised.

If the College uses IT systems to make automatic decisions based on personal data individuals have a right to object and:

- request human intervention in the decision making
- be able to express their point of view
- obtain an explanation of how a decision has been reached
- challenge the decision

This right does not exist if the automated decision making:

- is necessary to fulfil a contract to which they are party
- is authorised by law
- the data subject has consented to the processing

Individuals also have the right to object to data being used for research purposes unless the research is being undertaken in the wider public interest which outweighs a data subject’s right to privacy.

Right to be Informed

The College issues a privacy notice which explains what information the College is processing, the legal basis for this, the purpose of processing, who the information is shared with and other information required by data protection legislation. The current privacy notice is available on the College’s website (www.uplandscc.com) or on request from the College office (01892 782135)

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child’s educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Biometric recognition systems

Where we use students’ biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The College will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parents/carers and students have the right to choose not to use the College’s biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can be given a swipe card to pay for school dinners at each transaction if they wish.
Parents/carers and students can object to participation in the College’s biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted. As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil’s parent(s)/carer(s).

Where staff members or other adults use the College’s biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the College will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the College site to ensure it remains safe. We will adhere to the ICO’s code of practice for the use of CCTV.

We do not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the ICT Support Manager.

13. Photographs and videos

As part of our College activities, we may take photographs and record images of individuals within our College.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don’t need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within College on notice boards and in College magazines, brochures, newsletters, etc.
- Outside of College by external agencies such as the College photographer, newspapers, campaigns
- Online on our College website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding policy for more information on our use of photographs and videos.
14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where the College’s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our College and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Whenever a new policy, procedure, system or database involving personal data is proposed a Data Protection Impact Assessment (DPIA) will be completed. This will be used to identify and reduce any risks to privacy and potential risks of harm to individuals through the misuse of their personal information.

The College also recognise that in some circumstances it will be mandatory to conduct a DPIA where processing is likely to result in a high risk to individuals.

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
Where personal information needs to be taken off site, staff must sign it in and out from the College office.

Passwords that are at least 8 characters long containing letters and numbers are used to access College computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.

Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for College-owned equipment (see our e-safety/ICT policy/acceptable use agreement).

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the College’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The College will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a College context may include, but are not limited to:

- A non-anonymised dataset being published on the College website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a College laptop containing non-encrypted personal data about students

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the College’s processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our College’s practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full Governing Board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Whistleblowing policy
- E-Safety policy
- Child Protection & Safeguarding policy
- ICT/Acceptable Use policy
Appendix 1: Uplands Data Breach Management Process

If you become aware of a personal data breach you should immediately notify via the appropriate escalation person;
- Notify Sophie Hanson as the GDPR Lead within the school.
  Sophie Hanson to refer the data breach to our ESCC DPO (Mr Peter Questier, Tel: 01273 337610, or email CS.DPA@eastsussex.gov.uk) as soon as they happen so that he can make an assessment of whether this needs reporting to the Information Commissioner’s Office (ICO).
- **Failure to report breaches that need to be reported to the ICO within 72 hours constitutes a breach so it is very important that the appropriate escalation person is made aware of breaches as soon as they happen.**
  - The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    o Lost
    o Stolen
    o Destroyed
    o Altered
    o Disclosed or made available where it should not have been
    o Made available to unauthorised people
  - The DPO will alert the Principal and the Chair of Governors
  - The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
  - The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
  - The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people’s rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    o Loss of control over their data
    o Discrimination
    o Identify theft or fraud
    o Financial loss
    o Unauthorised reversal of pseudonymisation (for example, key-coding)
    o Damage to reputation
    o Loss of confidentiality
    o Any other significant economic or social disadvantage to the individual(s) concerned
  - If it’s likely that there will be a risk to people’s rights and freedoms, the DPO must notify the ICO.
  - The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school’s computer system.
  - Where the ICO must be notified, the DPO will do this via the ‘report a breach’ page of the ICO website within 72 hours. As required, the DPO will set out:
    o A description of the nature of the personal data breach including, where possible:
      ▪ The categories and approximate number of individuals concerned
      ▪ The categories and approximate number of personal data records concerned
    o The name and contact details of the DPO
    o A description of the likely consequences of the personal data breach
A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

Questions to consider when assessing level of risk:

- Nature of the breach? Category and amount of individuals affected? What are the potential adverse consequences? How likely are these? What could the data tell a 3rd party, what harm could this cause?
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO.

  For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches, its effects and any remedial action taken will be recorded by Sophie Hanson, GDPR Lead, and stored on the school’s computer system.

The DPO, Principal and GDPR Lead will meet to review how the breach was caused, even in part, by inadequate policies or a lack of a clear allocation of responsibility for example and take remedial action. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

Uplands will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
• The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach to consider:
• Ensure details of pupil premium interventions for named children are not published on the school website
• Ensure only anonymised pupil exam results or staff pay information is being shared with governors
• A school laptop containing non-encrypted sensitive personal data being stolen or hacked
• The school’s cashless payment provider being hacked, and parents’ financial details stolen
Appendix 2 Third Party Requests for Information

From time to time, Uplands Community College will get requests for information from third parties, such as children’s social services, the police and other schools. This information may be needed in order to investigate a potential crime or an alleged child protection incident or may be due to a student moving schools temporarily or permanently. When processing a third-party request for information we must exercise due diligence and caution.

The Data Protection Act 2018 Schedule 8, Part 4 ("Safeguarding of children and of individuals at risk") states that the processing of personal data can be carried out without consent if it is necessary to "protect an individual from neglect or physical, mental or emotional harm, or to protect the physical, mental or emotional well-being of an individual", (Schedule 8, Part 4.1.a.iii). It also states that personal data can be processed in relation to safeguarding without consent in the following situations:

- If it is not possible for the data subject to consent (Schedule 8, Part 4.2.a)
- If it is not possible for the data controller (i.e. the school) to gain consent from the data subject (Schedule 8, Part 4.2.b)
- If gaining consent from the data subject would impact on their physical, mental or emotional health so is not possible (Schedule 8, Part 4.2.c)

When there is a concern that a child is at risk of significant harm, all requested information held by Uplands Community College must be shared with Children’s Social Care, police and health professionals; as directed by:

- Section 47 of the Children Act 1989
- Sections 10 and 11 of the Children Act 2004
- GDPR Article 6.1(c) (Legal obligation)

Records may also be shared in:

- **court cases** where a solicitor or other third party is requesting information **without** a court order - legal advice should be sought.
- Where a judge **makes** a court order requesting information be shared – legal advice should be sought.
- School-to-school transfers – consent should be given.


**When and how to share information**

When asked to share information, you should consider the following questions to help you decide if, and when, to share. If the decision is taken to share, you should consider how best to share the information.

**When**

**Is there a clear and legitimate purpose for sharing information?**

- Yes – see next question
- No – do not share
Do you have consent to share?
• Yes – you can share but should consider how
• No – see next question

Does the information enable an individual to be identified?
• Yes – see next question
• No – you can share but should consider how

Have you identified a lawful reason to share information without consent?
• Yes – you can share but should consider how
• No – do not share

How
• Identify how much information to share
• Distinguish fact from opinion
• Ensure that you are giving the right information to the right individual
• Ensure where possible that you are sharing the information securely
• Where possible, be transparent with the individual, informing them that that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual. All information-sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage you are unsure about how or when to share information, you should seek advice on this. You should also ensure that the outcome of the discussion is recorded. In order to ensure that such requests are processed effectively, the following guidelines should be followed. The request for information is likely to come directly to the pastoral team, or to the main school reception. The person receiving the request should follow point 1.

The person who is given the request to process should follow points 2 to 15.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Pass the request to the most appropriate person within 24 hours of receiving the request with the correct permissions. Speak directly to the person to ensure that they know the request exists. If they are absent, pass the request directly to their line manager.</td>
</tr>
<tr>
<td>2.</td>
<td>Check that the request for information has come from a legitimate source. If the person is not known to the school, the request should be submitted in writing.</td>
</tr>
<tr>
<td>3.</td>
<td>Ensure that the appropriate permissions have been given by the owner of the data, or their parent. There should be written evidence of the consent.</td>
</tr>
<tr>
<td>4.</td>
<td>Make a note of the date that the request was passed on and the person who the request was passed to.</td>
</tr>
<tr>
<td>5.</td>
<td>Apply the questions in the ‘When and how to share information guidance’ given above to ensure that the information should be shared.</td>
</tr>
<tr>
<td>6.</td>
<td>If the information should be shared, follow the points 7 to 15. If the information shouldn’t be shared, contact the person who has requested the information to explain why the information will not be provided. If this is done in writing, a copy of the correspondence should be kept. If this is done by telephone, a contemporaneous transcript of the conversation should be made and it should be dated, signed and filed.</td>
</tr>
<tr>
<td>7.</td>
<td>For a routine request for information (eg for a school-to-school transfer, or a request from social services for information regarding a current safeguarding investigation), inform your line manager of the request and your decision regarding sharing the information. If the request involves a potential safeguarding issue, the DSL should also be informed.</td>
</tr>
<tr>
<td>8.</td>
<td>For a non-routine or unusual request, or for a request for information about a student who left more than 2 years previously, or for a request that may directly involve a member of staff or former member of staff, the Principal, SHA and the DSL (by email) should all be informed unless the agency has a</td>
</tr>
</tbody>
</table>
specific and relevant reason why one or more of the specified people should not be informed. In the unlikely event that none of the specified people are allowed to be informed, advice should be sought from the Chair of Governors. If you are in any doubt about whether it is a routine or non-routine request, seek advice from your line manager.

9. Only information that is directly relevant to the request and for which there is clear consent or legal authority should be shared. Advice can be sought from the DSL, SHA or the Principal if required.

10. Collate the requested information in a timely fashion, usually no more than 28 days from being passed the request. Likely sources of information include:
   - Student file
   - SIMS
   - Emails
   - SEN file
   - Safeguarding file
   - Current or previous staff - a written record of any conversation should be kept. This record is for internal school purposes.
   
   If the student has left the school, SHA should be contacted so that the archive information can be checked.

11. Information should be read to see if any redaction is necessary to protect the confidentiality of other parties. If the information is being requested by the police, full disclosure of information may be required. Clarification should be sought from the requesting police officer and advice sought from SHA if necessary.

12. All of the relevant information should be copied. In most situations the copy should be sent to the agency that has requested the information. In some situations, the police may need the original documents, in which case the copy should be kept in school.

13. Copies should be taken and filed of any other information such as forms requested before being sent to the requesting agency.

14. The 'Third-Party Request for Information' form at the end of this document should be completed and put in the student file. In the event that the student has left school and the file is no longer in school, the form should be given to SHA for filing.

15. A record of the date of posting should be made. If the information is sensitive, the method of sending the information should be carefully considered, and secure email or recorded delivery may be necessary. Please the policy for data in transit (staff handbook, policy folder) for further information, or ask SHA for advice.

The form on the following page should be completed in the event of information being shared and kept in the student’s file.
Third Party Request for Information

Name of agency requesting the information ..........................................................................................................................
Name of the person requesting the information ......................................................................................................................
Date of request ........................................................................................................................................................................
Date line manager and/or DSL informed ...............................................................................................................................  
Information requested ...................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
 ..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
Information shared: Yes / No (please circle)  
Reason for decision   
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
Consent sought Yes / No (please circle)  
If No, give reason   
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
..........................................................................................................................................................................................
Date information shared if applicable ........................................................................................................................................
Method of sharing ........................................................................................................................................................................
Date form completed ...................................................................................................................................................................
Name of person completing the form ........................................................................................................................................
Signature  
.............................................................................................................................................................................................